PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-332019

(43)Date of publication of application : 30.11.2001

---

(51)Int.Cl. G11B 20/10

---

(21)Application number : 2000-144456 (71)Applicant : TAIYO YUDEN CO LTD

(22)Date of filing : 17.05.2000 (72)Inventor : OMURA YUKIHIDE
SUNAKAWA RYUICHI
SHIMIZU HIRONOBU

---

(54) DATA RECORDING AND REPRODUCING METHOD FOR WRITE-ONCE TYPE OPTICAL DISK, DATA REPRODUCING DEVICE FOR WRITE-ONCE TYPE OPTICAL DISK AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data recording and reproducing technique for a write- once type optical disk which can surely prohibit the reutilization of plaintext data after decoding without expecting the morality on a reproducing side user and can therefore assure the security in all stages from recording to reproducing.

SOLUTION: In writing data to the write-once type optical disk, the data is written by adding a prescribed confidential flag to the data and when the writing data is reproduced, the presence or absence of the confidential flag is inspected. When the presence of the confidential flag is detected, the operation relating to the formation of the copy of the data is restricted. The reutilization of the reproduced data may be

obstructed and the security in the reproduction stage assured.

LEGAL STATUS [Date of request for examination] 02.10.2003
[Date of sending the examiner's decision of rejection] 12.10.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2006-025514
[Date of requesting appeal against examiner's decision of rejection] 10.11.2006
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The data-logging playback approach for write-once mold optical disks characterized by to include the duplicate limit process of restricting the actuation about generation of the duplicate object of said data when reproduce said write-in data, and the existence of said secret flag inspects and existence of a secret flag is detected [the write-in process which adds and writes a secret predetermined flag in said data in case data are written in a write-once mold optical disk, and].
[Claim 2] The data-logging playback approach for write-once mold optical disks according to claim 1 characterized by providing further the access-restriction process which restricts access to this optical disk based on the security information stored in the system area of said optical disk.
[Claim 3] The data regenerative apparatus for write-once mold optical disks characterized by having a judgment means to judge whether the secret predetermined flag is contained in the data read from the write-once mold optical disk, and a prohibition means to forbid the actuation about generation of the duplicate object of said data when existence of a secret flag is judged by this judgment means.
[Claim 4] The record medium characterized by storing the program for realizing a judgment means to judge whether the secret predetermined flag is contained in the data read from the write-once mold optical disk, and a prohibition means to forbid the actuation about generation of the duplicate object of said data when existence of a secret flag is judged by this judgment means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the data-logging playback approach for write-once mold optical disks, a data regenerative apparatus, and a record medium. It is related with the data-logging playback approach, data regenerative apparatus, and record medium which are applied to the write-once mold optical disk represented in detail by CD-R (Compact Disc Recordable) which can write in data only once.
[0002]
[Description of the Prior Art] CD-ROM (Compact Disc Read Only Memory) is used abundantly at the distribution medium of electronic data, such as various contents and a computer program. the optical disk unit of the write-once (postscript is possible) mold as for which elimination or overwrite of data are not made to little sample version CD and private CD of the number of distribution (the number of manufactures) although CD-ROM is a duplicate object manufactured by press molding etc. from the master CD which recorded electronic data and it is mainly used for the media of large quantity distribution -- CD-R is used typically. CD-R has the difference on CD-ROM and structure between transparent disk substrates and reflecting layers (detailed structure is mentioned later.) in that it has the recording layer which consists of organic coloring matter, irradiates high power laser at the recording layer concerned using the recording device (CD-R writer) of dedication, and can record information in a user phase by forming an information pit in the recording layer concerned by the thermal reaction.
[0003] CD-R is the record medium of the write-once mold which cannot perform elimination or overwrite of data as above-mentioned. That is, elimination and rewriting of data which were written in once are impossible. Therefore, since it has the

outstanding advantage that elimination and the alteration of data by the inaccurate person can be prevented certainly, the position as a record medium indispensable to applications, such as storage of electronic data which requires especially secrecy, and distribution, today has been established, but on the other hand, although read-out of recording information of CD-R is free therefore, it also has the fault that informational unjust read-out or an informational illegal copy cannot be prevented.

[0004] Then, what is enciphered and recorded in case the data which require secrecy are recorded, for example, as shown in drawing 16 is performed. In drawing, the plaintext data 100 are data of the "student" before encryption, for example, are data of the text format which has readability. When invisibility-izing this plaintext data 100 and recording it, it changes into the encryption data 102 first using the predetermined encryption tool 101. Although especially the method of encryption is not limited, it is a common key system using a key common to a cryptographic key and a decode key. Hereafter, on behalf of this key, it is made a "cryptographic key." Therefore, when you tell a cryptographic key to below, suppose that a decode key is also meant.

[0005] Now, the enciphered data (it sets to drawing and is the encryption data 102) are invisible data, since they are insurance (in computational complexity insurance) even if it distributes them as it is, by writing this encryption data 102 in CD-R103, can prevent unjust reading of data and can maintain security. In the case of playback, if the encryption data 104 are read from CD-R1 and it returns to the plaintext data 106 using the predetermined decode tool 105, it is good (if it decodes).

[0006]

[Problem(s) to be Solved by the Invention] However, if it is in the above-mentioned security countermeasures, reuse of the data after decode (plaintext data 106) is free, and the inconvenience of being obtained only in the condition of having been chiefly stored in CD-R103 has the effectiveness of data integrity. That is, about the plaintext data 106 after being read from CD-R103 and decoding, security did not start at all but the data integrity to this plaintext data 106 had the trouble that a playback side user's morals only had to be expected.

[0007] therefore -- without it expects from a playback side user's morals the technical problem which this invention tends to solve -- reuse of the plaintext data after decode -- certain -- forbidding -- with -- **** -- it is in offering the data-logging playback technique for write-once mold optical disks in which the security of all the phases from record to playback is securable.

[0008]

[Means for Solving the Problem] The data-logging playback approach according to

claim 1 for write-once mold optical disks is characterized by to include the duplicate limit process of restricting the actuation about generation of the duplicate object of said data, when reproduce said write-in data, and the existence of said secret flag inspects and existence of a secret flag is detected [the write-in process which adds and writes a secret predetermined flag in said data in case data are written in a write-once mold optical disk, and]. According to this, if a secret predetermined flag is detected at the time of playback of data, generation of the duplicate object of playback data will be restricted. The data-logging playback approach for write-once mold optical disks according to claim 2 is characterized by providing further the access-restriction process which restricts access to this optical disk based on the security information stored in the system area of said optical disk in the data-logging playback approach for write-once mold optical disks according to claim 1. According to this, based on the security information stored in the state of invisibility, access to an optical disk is restricted to the system area of an optical disk. The data regenerative apparatus for write-once mold optical disks according to claim 3 is characterized by having a judgment means to judge whether the secret predetermined flag is contained in the data read from the write-once mold optical disk, and a prohibition means to forbid the actuation about generation of the duplicate object of said data when existence of a secret flag is judged by this judgment means. According to this, if a secret predetermined flag is detected at the time of playback of data, generation of the duplicate object of playback data will be forbidden. A record medium according to claim 4 is characterized by storing the program for realizing a judgment means to judge whether the secret predetermined flag is contained in the data read from the write-once mold optical disk, and a prohibition means to forbid the actuation about generation of the duplicate object of said data when existence of a secret flag is judged by this judgment means. According to this, said judgment means and a prohibition means are realized by organic association with the hardware resource and this program containing a microcomputer.

[0009]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail with reference to a drawing. In addition, instantiation of the notation of the specification thru/or example and numeric value of various details in the following explanation, or a character string and others is reference to the last for making thought of this invention clear, and it is clear that its the thought of this invention is not limited by those all or parts. Moreover, although the explanation covering the details is avoided about Following "a circumferential governor term"

term The well-known technique, a well-known procedure, well-known architecture, and well-known circuitry, this is also for giving explanation brief and does not eliminate intentionally all or a part of these Governor Shu term. Since it is this the Shu Governor term at the application event of this invention and this contractor can just be going to know it, naturally it is contained in the following explanation.

[0010] First, the utilization gestalt of the write-once mold optical disk (henceforth "CD-R") of this operation gestalt is explained roughly. Drawing 1 is the utilization mimetic diagram of CD-R1 of this operation gestalt. Three phases, the manufacture phase of CD-R1 by the manufacturer (manufacturer), the record phase of data of requiring the secrecy to CD-R1 concerned by User A, and the playback phase that reads data from recorded CD-R1 concerned by User B, and is reproduced, are shown by this drawing.

[0011] Although it becomes clear also from next explanation, in (1) manufacture phase, the identification information (henceforth "ID information") of a proper and the cryptographic key (what serves as a decode key) in a predetermined cipher system are electronically recorded on CD-R1, and are shipped to CD-R1. The record location of ID information and a cryptographic key is a location (system area; about field structure, it mentions later.) where direct access from a user is not permitted. (2) Judge whether it is that (henceforth a "support disk") from which CD-R1 concerned was made from ID information on the CD-R1 by a predetermined manufacturer or the predetermined manufacturer registered beforehand in the record phase. When it is a support disk, while adding predetermined "secret flag" to record data, record data (what added the secret flag) are enciphered using the cryptographic key currently written in CD-R1, and the encryption data is recorded on CD-R1. (3) While carrying out user authentication using ID information on CD-R1 and approving decode processing of encryption data only to a registered user (user who knows ID information), when reusing duplicate processing of a decode copy of data, preservation, etc. by performing, judge the existence of "the secret flag" in record data, and, in with a secret flag, carry out [reuse / above-mentioned] forcible interruption in refusal, for example, copy actuation and preservation actuation, in a playback phase.

[0012] In these three phases, the device for giving security to CD-R1 ** ID information and a cryptographic key were written in the system area of CD-R1 at the time of manufacture, ** At the time of record by User A, "the secret flag" was added to record data, ** Record data (with a secret flag) are enciphered at the time of this record, and it was made to write in CD-R1. ** At the time of playback by User B, user

authentication using ID information is performed and decode of encryption data was permitted only to the registered user, ** When reuse of decode data is performed at the time of this playback, be in judging the existence of a secret flag and having been made to carry out forcible interruption of the reuse actuation in with a secret flag.

[0013] ** ID information is used for the user authentication at the time of data playback, and the cryptographic key of ** is used for the decode of encryption data performed by a data encryption and the registered user. These ID information and cryptographic keys are the "hiding data" which were written in the field (system area) to which user access is not permitted among the record sections of CD-R1 and which were invisibility-ized so to speak. ** ID information is used also for the judgment of the support disk at the time of data writing again. As aforementioned, a support disk is CD-R1 made by a predetermined manufacturer or the predetermined manufacturer registered beforehand, and means in accuracy that it is the special disk (CD-R1) "supported" the cure against reuse prohibition of the data after decode performed using "a secret flag."

[0014] Here, a secret flag may be data of a flag format as the identifier, and may be another formats other than a flag. The point that it should mind is to have to secrecy-ize existence of a secret flag (or what is equivalent to a secret flag) to a user. Since a possibility that the location of a flag may be detected generally cannot be denied when investigated as a round robin although the data of a flag format are 1 bit data of a binary logic (it is also called a boolean mold.) and temporary secrecy-izing is possible by making the bit position secret, it is desirable to consider as the data which took a positive cure against secrecy-ized like digital watermarking desirably. Digital watermarking means what predetermined message information is hidden in one or more domains of the frequency of the original data, space, or time amount for (it embeds), without spoiling the quality of original data. A secret flag is used in a playback phase as a check flag for forbidding reuse (plaintext data being copied and saved at other record media; it also being called duplicate actuation.) of the plaintext data after decode. without it can also take the security countermeasures of the plaintext data after decode and is dependent on the morals of the playback side user who is the technical problem of the invention in this application in addition to the security of CD-R1 by encryption data by this -- reuse of the plaintext data after decode -- it can forbid -- with -- **** -- the write-once mold optical disk which can secure the security of all the phases from record to playback can be offered.

[0015] Hereafter, an example is given and explained about a configuration and an operation required for the above-mentioned technical-problem achievement. Drawing

2 is the external view (a) and its important section enlarged drawing (b) of CD-R1 in this operation gestalt. Setting to these drawings, CD-R1 is the diameter of 12cm (there is also a thing with a diameter of 8cm.). Hereafter, it is a thing with a diameter of 12cm and explains. It has the shape of a disk and with a diameter of 15mm center hall 1a is formed in the core of a disk. The distance from the core T0 of a disk to the wall (disk common-law marriage T1) of center hole 1a 7.5mm, The distance from T0 to the disk rim T7 is 60mm. Among these T1-T7 Two or more concentric record sections, That is, they are PCA (Power Calibration Area), PMA (Program Memory Area), and a lead-in groove (it has abbreviated to "RI" by a diagram.) to the order from the inner circumference side of a disk. Data area (it has abbreviated to "UA" by a diagram.) And lead-out (it has abbreviated to "RO" by a diagram.) Each field is prepared.

[0016] When each field is outlined, PCA located in T2 - T3 is a trial writing field for the laser adjustment on the strength performed in case data are recorded on CD-R1. Generally about 100 times of this trial writing are possible, and it consumes the field of one batch by at least 1 time of data logging. PMA located in T3 - T four is a field where the track number and initiation/termination location are saved temporarily, when there is a truck of the session which is not closed yet by CD-R1. The lead-in groove (RI) located in T-four-T5 is a field in the head (inner circumference side of a disk) of a session truck, and is a field where TOC (the number of trucks currently recorded on Table OfContents:CD, a starting position, and the die length of the sum total of a data area) of a session is saved. A closing of a session writes the information saved at PMA temporarily in this lead-in groove (RI).

[0017] The data area (UA) located in T5-T6 is a field in which data are actually written in a user phase. The storage capacity of data is about 680 M bytes (a thing with a diameter of 8cm a maximum of about 190 M bytes) of max, and if this storage capacity is expressed with sound recording time amount, it will become in the maximum about 74 minutes (a thing with a diameter of 8cm a maximum of about 21 minutes). a data area (UA) is managed by the logical block of the predetermined size (2 K bytes) unit which continues from immediately the back of a lead-in groove (RI) -- having -- coming -- **** -- every logical block -- a maximum of [0 to] -- LBN (Logical Block Number) to about 330000 is assigned. The lead-out (RO) located in T6-T7 is a field in the last (periphery side of a disk) of a session, and is a field which shows that the last of a data area (UA) was reached.

[0018] The location on the disk of each [these] field is standardized except for T3. That is, the location where T2 separated from T0 22.5mm, the location where T four separated from T0 23mm, the location where T5 separated from T0 25mm, and T6 are

prescribed to become the location distant from T0 58mm. In addition, although the same sign (T7) shows the disk rim and the termination location of lead-out (RO) by a diagram, this is the convenience of a graphic display. The actual termination location of lead-out (RO) turns into a location distant from T0 58.5mm. The following, as long as there is no notice, T7 shall express the termination location of lead-out (RO). Incidentally, initiation and the termination location (T6 and T7) of lead-out (RO) change according to the amount of the data recorded on CD-R1. The above-mentioned actual value (T6=58mm, T7=58.5mm) is a thing when making the amount of stored data into max.

[0019] Drawing 3 is cross-section structural drawing of CD-R1. CD-R1 is transparent, on substrate 1b which consists of an ingredient (for example, plastics) which was excellent in thermal resistance, moisture resistance, and a moldability, and was equipped with necessary optical properties (a refractive index, birefringence, etc.), carries out the laminating of the protective layer 1e which consists of hard material, such as 1d of reflecting layers, resin, etc. which consist of metallic materials, such as recording layer 1c which consists of organic coloring matter, and aluminum, and is formed. The thickness of the whole cross section is 1.2mm.

[0020] The point that the point of having recording layer 1c, and 1f of spiral guide rails called a wobbles groove between recording layer 1c and substrate 1b are formed has the difference in structure with CD-ROM. Record of the data to CD-R1 irradiates the powerful laser for record along with 1f of guide rails from the background of substrate 1b, and is performed by heating recording layer 1c and forming an information pit (Pit: a part for the physical deformation affected zone for modulating the laser reflected light for playback). 1f of guide rails is continuously formed toward the periphery side (from a periphery side to or an inner circumference side) in the way of a picture drawn without lifting the brush from the paper from the inner circumference side of a disk, the width of face of 1f of guide rails is about 0.5-0.7 micrometers, and spacing is about 1.6 micrometers. Data logging in a user phase is performed along with 1f of guide rails by forming an information pit in recording layer 1c of a guide rail 1f (or land between 1f of guide rails) directly under. In addition, although it sees from the background of CD-R1, a part for a land (crest) and a crevice is called groove (trough) for a part for heights of 1f of guide rails and the part of a trough is generally called wobbles group, a crest and a trough are not distinguished on these descriptions.

[0021] Here, the role of 1 of 1f of guide rails is to hold the timing information for controlling the rotational speed of a disk at the time of data logging of a user phase. 1f of guide rails is formed in the configuration which moves in a zigzag direction with a

predetermined period (for example, period equivalent to 22.05kHz) (it is also called "wobbling".) for this role. At the time of record of data, the optical pickup at the time of data logging and the relative velocity between disks are kept constant by tracing this meandering by the optical pickup, detecting a period, and controlling the rotational speed of a disk so that that detection period becomes fixed. Other roles of 1f of guide rails are to hold various disk information including the positional information of each record section on a disk (PCA, PMA, RI, UA, and RO). Disk information is also called ATIP (Absolute Time In Pregroove: call it a common name "A chip".), and various information other than the above-mentioned positional information, such as the record laser reinforcement and disk rotational speed of criteria, an application code, or a disk type, is included in ATIP.

[0022] Drawing 4 is the format conceptual diagram of each record section of CD-R1. In this drawing, PCA, PMA, a lead-in groove (RI), a data area (UA), and lead-out (RO) correspond to the same name part in drawing 2 (b), respectively. Although especially the size (information write-in possible capacity) of PCA and PMA is not decided, about 3.5 M bytes is secured by the initial complement corresponding to the above-mentioned count of trial writing (generally about 100 times), or the count of the memory of session information, for example, PCA, and the capacity of about 2 M bytes is secured by PMA. Incidentally, the starting position (T2) of PCA and the starting position (T3) of PMA can be expressed in writing from such instantiation capacity with the location for "T2=T-four-about 35 seconds", and the location for "T3=T-four-about 13 seconds" on the basis of the starting position (T four) of the standardized lead-in groove (RI).

[0023] Since it is a trial writing field at the time of PCA performing data logging, and the field which stores temporarily the session information by which PMA is not closed as stated above, these two fields (PCA/PMA) are fields used only at the time of data logging (access). On the other hand, since it is the field which records as TOC the session information by which the lead-in groove (RI) was closed, the field where, as for a data area (UA), data are written in actually, and the field where lead-out (RO) specifies the end of a data area, these three fields (a lead-in groove / data area / lead-out) are fields used at both times of data logging and playback (access).

[0024] On the other hand, if all these fields are seen in respect of the access ease from a user that is The reader of CD-R1 If it evaluates in respect of the ability of the content of storage to be easily accessed using the usual tools (file system on the operating system typically carried in the personal computer concerned etc.) from users, such as a personal computer which it had Although complete grasp of the

content of storage is possible though natural about a data area (UA), content grasp of other fields (PCA, PMA, a lead-in groove, and lead-out) is impossible.

[0025] Of course, since such a tool is difficult to receive for a general user, if it is possible if a special tool is used, but utilization of the exceptional tool to apply is removed, it can be said that other fields other than a data area (PCA, PMA, a lead-in groove, and lead-out) are special fields where only access from a system was permitted. On these descriptions, this special field is called "system area" and the thing of the field where access from a user was permitted is called "user area." That is, a user area, other PCA, PMA, a lead-in groove (RI), and lead-out (RO) of a data area (UA) are system areas.

[0026] The proper information on CD-R1 (henceforth "ID information") and predetermined cryptographic key information are written in a part of system area in a manufacture phase as CD-R1 in the gestalt of this operation was explained previously. Although it is desirable to have a unique value (value not overlapping) covering the total number of manufactures of CD-R1 as for ID information, since there is concern whose information bit forms many bits and presses the storage capacity of a system area when the number of manufactures becomes huge, it is good also as different information for every manufacture lot, every production line, and every manufacture stage.

[0027] This ID information is used for access collating to CD-R1 in a user phase so that it may mention later. For example, the input of ID is required with the application which reproduces data, coincidence with inputted ID and ID currently written in the system area is judged, and, only in coincidence, access is permitted. The playback and the duplicate of data by the inaccurate user (user who does not know ID) can be prevented by this, and runoff of data and the appearance of an inaccurate product can be avoided.

[0028] Advice to the user of ID information written in CD-R1 must be performed to every [of each CD-R1] purchaser (or normal acquisition person). For example, if ID information written in a certain CD-R1 (it considers as "Disk A" for convenience hereafter.) is assumed to be "abcdef", the means of a document thru/or others will notify the ID information ("abcdef") concerned to the purchaser or normal acquisition person of Disk A. As this means, the slip which indicated the ID information ("abcdef") concerned may be put in into the package (plastics case which stored Disk A) of Disk A, for example, and you may tell orally at the time of the purchase of Disk A etc. In addition, what is necessary is just to be, able to transmit to a user ID information written in CD-R1 at the time of shipment in short at accuracy, although various

means can be considered.

[0029] The key information written in a system area together in a manufacture phase on the other hand is used in order to encipher the raw data written in a data area in a user phase. That is, after reading a cryptographic key with the application which records data and changing raw data into encryption data using this cryptographic key, that encryption data is written in the data area of CD-R1. Also in case this cryptographic key decodes encryption data, it is used. That is, the input of ID is required with the application which reproduces data at the time of playback of data, coincidence with inputted ID and ID currently written in the system area is judged, in coincidence, a cryptographic key and encryption data are read, encryption data are decoded using the cryptographic key, it changes into raw data, and utilization of a user is presented.

[0030] Therefore, the inaccurate user who does not know ID Since the access to data itself is refused, while reading of inaccurate data is avoidable In the usual technical information, even if access is successful with a certain means, since access to the cryptographic key written in the system area is impossible, it should not decode encryption data to raw data, but should devise a thoroughgoing security step in this point.

[0031] Drawing 5 is instantiation structural drawing of the data format containing ID information written in a system area, and a cryptographic key. In this drawing, the first example (a) has the magnitude of 20 bytes by all that consisted of each information on 8 bytes of ID information, 8 bytes of DES (Data Encryption Standard: U.S. federal government standard code specification) cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date. Moreover, the second example (b) has the magnitude of 36 bytes by all that consisted of each information on 8 bytes of ID information, 24 bytes of Triple DES cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date. It is decided by whether the dependability of a cryptographic key is thought as important chiefly, or storage capacity pressure of a system area is avoided whether to adopt format [which]. In addition, the byte count of a graphic display, the class of cryptographic key, and format structure are instantiation to the last. What is necessary is just to, write the information (ID information) in which solid-state discernment of CD-R1 is possible, and the key information on predetermined [which can both be decoded from encryption data to raw data] (cryptographic key) which can change raw data into encryption data in the system area of CD-R1 in short.

[0032] Drawing 6 is the rough block block diagram of a write-once mold optical disk

record regenerative apparatus (henceforth a "CD-R record regenerative apparatus"). The spindle motor 12 which this CD-R record regenerative apparatus 10 supports the clamping area (information non-recording area prepared among T1-T2 of drawing 2 (a)) of CD-R1, and carries out revolution actuation in the predetermined direction, The optical pickup 14 which spaces substrate 1b of CD-R1, and irradiates the object for record, or the laser 13 for playback (generally infrared laser with a wavelength of 770-830nm) at recording layer 1c, While having the coarse adjustment motor 15 made to move an optical pickup 14 to radial [of a disk] in harmony with the seeking motor which is not illustrated [which was prepared in the interior of an optical pickup 14] The disk roll control section 16 which controls the rotational speed of a spindle motor 12, The rotational speed of the coarse adjustment motor 15, and the coarse adjustment motor control section 17 which controls a hand of cut, The pickup control section 18 which performs control of the location of an optical pickup 14, or laser reinforcement, It has playback/record control section 19 which controls the reading signal from an optical pickup 14, conversion of waveform of the write-in signal to an optical pickup 14, etc., and has further the controller 20 which generalizes each of these control sections.

[0033] the CD-R record regenerative apparatus 10 is built in the expansion slot of the host equipments 21, such as a personal computer, (or it carries out external -- having), connects between host equipment 21 and controllers 20 by cable 21a of predetermined signal specification (for example, SCSI:Small Computer System Interface), and is used.

[0034] The CD-R record regenerative apparatus 10 which has such a configuration can perform record and playback of recording information of the information on CD-R1 as it is shown below. in addition, CD-R1 -- CD-ROM -- although it is a compatible device and information playback of CD-ROM is also possible for the CD-R record regenerative apparatus 10, since there is no direct relation, explanation is abbreviated to this invention.

[0035] If the application program only for CD-R records (henceforth a "lighting program") is executed with <record actuation of information on CD-R1> host equipment 21, the laser on-the-strength calibration command from a lighting program will be first told to a controller 20. While a controller 20 answers this command, tells a necessary command to each control section and locating an optical pickup 14 in an PCA sky field (field which is not tried, written and carried out) of CD-R1 After controlling rotational speed of a spindle motor 12 (it controls so that the relative velocity in the current position of an optical pickup 14 turns into a predetermined

rate), the laser 13 for record of provisional reinforcement (arbitration power between 5.5-8mW) is irradiated from an optical pickup 14 to an PCA sky field, and trial writing is performed. Position control of an optical pickup 14 and rotational-speed control of a spindle motor 12 are performed according to the information (timing information and ATIP information) reproduced from the trace signal of 1f of guide rails of CD-R1.

[0036] Subsequently, a controller 20 reads the data written [were tried and] and set to PCA through playback/record control section 19, and returns the data to the lighting program of host equipment 21. A lighting program is tried, writes, compares data with expected value, judges the propriety of laser reinforcement, and if a judgment result is "**" while carrying out increase and decrease of the laser reinforcement of accommodation and publishing a laser on-the-strength calibration command again, if a judgment result is "no", it will start record actuation of the information on CD-R1.

[0037] This record actuation transmitting the necessary record data chosen suitably to a controller 20 from a lighting program, and performing the roll control of a spindle motor 12, and position control of an optical pickup 14 through each control section under control of this controller 20 by the user, while modulating the laser 13 for record from an optical pickup 14 by the above-mentioned record data, it records on the data area of CD-R1. And if record is completed, while writing TOC of closing and its session information for all sessions in a lead-in groove (RI), lead-out (RO) is formed after the last session.

[0038] In case the recording information of <playback actuation of recording information of CD-R1> CD-R1 is reproduced, the above-mentioned lighting program is unnecessary. However, the kind of the driver software for performing the interconversion of the file system of CD-R1 and the file system of host equipment 21 is indispensable. By using the CD-R record regenerative apparatus 10 through this driver software, a user can access the file system of CD-R1, without being conscious of distinction with other storage devices, such as a hard disk with which host equipment 21 was equipped. That is, since the file structure recognized by the file system of an operating system is in sight of a user, a user can use the file stored in other storage devices, and the file made into the object in CD-R1 in the same procedure.

[0039] While the CD-R record regenerative apparatus 10 reads the TOC information in a lead-in groove (RI) and provides the driver software of host equipment 21 with it on the occasion of this file access When the read-out command of a specific file is received from the driver software concerned While specifying the truck of a data area

(UA) with which the data of the file concerned were written in with reference to the TOC information in a lead-in groove (RI) and locating an optical pickup 14 in the starting position of the truck Control the rotational speed of a spindle motor 12, irradiate the laser 13 for playback (the point that power is stopped by about 0.2mW is removed, and it is the same as the laser for record) from an optical pickup 14 at CD-R1, and the file data concerned is read. A series of actuation of transmitting the reading data to host equipment 21 is performed.

[0040] Thus, the CD-R record regenerative apparatus 10 can also perform playback of the information written in CD-R1 while being able to write in information on CD-R1. Although this CD-R record regenerative apparatus 10 is an indispensable component when writing in information on CD-R1 in a record phase, it is a playback phase and is a component needed also when reproducing information written in CD-R1. CD-R1 -- CD-ROM -- it is a compatible device, the CD-ROM regenerative apparatus is carried in most, such as a personal computer of these days, it is possible to perform information playback of CD-R1 using that CD-ROM regenerative apparatus, and since this CD-ROM regenerative apparatus cannot be accessed at ID information or the cryptographic key which were written in the system area of CD-R1, also when reproducing too information written in CD-R1, the CD-R record regenerative apparatus 10 is an indispensable component.

[0041] Moreover, although the CD-R record regenerative apparatus 10 is equipment chiefly used by the record and the playback by the user, if it takes notice of the information write-in function to CD-R1, since it is applicable also to the writing of ID information or a cryptographic key performed in the manufacture phase of CD-R1, the fundamental actuation will go ahead with the talk by the following explanation as what is used in both a user phase and a manufacture phase in the above-mentioned CD-R record regenerative apparatus 10.

[0042] Information record processing > drawing 7 is a flow chart which shows the write-in actuation (it says below, "it is information record processing at the time of shipment".) of ID information and a cryptographic key in the manufacture phase of CD-R1 at the time of < shipment. In addition, in order to use only the record function of the CD-R record regenerative apparatus 10 in a manufacture phase, in the flow chart of a graphic display, the thing of the CD-R record regenerative apparatus 10 is called the "record machine" for convenience. However, not only the CD-R record regenerative apparatus 10 but the intention of the purport which may be the "record machine" only for manufacture phases is included in this vocabulary (record machine).

[0043] In drawing, if information record processing is started at the time of shipment,

first, non-recorded CD-R1 (a "disk" is called in a flow.) will be prepared, and a record machine will be loaded with this CD-R1 (step S11). next, host equipment 21 -- operating it -- the recording information to CD-R1 -- a manual entry -- or it generates automatically (step S12). This recording information is ID information on CD-R1, a predetermined private key, a date (creation data) on the day, etc., and that format is as being shown in drawing 5 (a) or (b).

[0044] Subsequently, if an information record instruction is published from host equipment 21 to a record machine (step S13), after a record machine answers this instruction, performs laser on-the-strength calibration processing and sets the laser 13 for record as proper power, it will carry out migration control of the optical pickup 14 in "the specific location" of the record section of CD-R1 (step S14). This specific location is an arbitration location on the field where direct access from a user is not accepted theoretically, i.e., the free space of a system area (PCA, PMA, a lead-in groove, or lead-out). It is an arbitration location (on a free space) on PCA currently especially recognized widely by this contractor preferably as a field where the existence is disregarded at the time of data playback, or PMA. Hereafter, let the above "a specific location" on [of explanation] expedient be an arbitration location on the free space of PCA.

[0045] Subsequently, modulating the laser 13 for record for recording information (information generated at step S12) using reception and its recording information from host equipment 21, it irradiates the laser 13 for record through transparent substrate 1b of CD-R1 at 1f of guide rails of recording layer 1c, forms an information pit in recording layer 1c of a guide rail 1f directly under, and a record machine performs the writing to CD-R1 of said recording information (step S15). The write-in starting position of recording information is the migration location of the optical pickup 14 performed at the above-mentioned step S14, i.e., the arbitration location on the free space of PCA, and the write-in termination location of recording information is a location which separated only the part equivalent to the size (it will be 20 bytes or 36 bytes if a format of drawing 5 is followed) of recording information from the location concerned.

[0046] Subsequently, a record machine reproduces recording information written in the system area by making into a playback termination location the location from which only the part equivalent to a playback starting position and the size of recording information separated the location concerned, and transmits this playback information to host equipment 21 while it returns an optical pickup 14 to the above-mentioned specific location. While judging that host equipment 21 was able to be normally written

in when comparison collating of the playback data and the above-mentioned recording information which were transmitted from the record machine was carried out, verification inspection was conducted (step S16) and both were in agreement and reporting that to an operator, it judges that writing went wrong and that is reported to an operator (step S17). In normal write-in information, an operator moves CD-R1 concerned to a shipment shelf (step S18), and, in write-in failure information, moves CD-R1 concerned to a defective shelf (step S19). And the above processing is repeatedly performed until prepared CD-R1 is lost (step S20).

[0047] Therefore, according to this "being information record processing at the time of shipment", hiding information, such as ID information, a cryptographic key, and creation data, can be written in the system area of non-recorded CD-R1, and it can ship to a commercial scene, and can send to a user. And in case data write-in processing, data regeneration, or disk copy processing in which it explains below is performed in a user phase, processing peculiar to the gestalt of this operation using the above-mentioned hiding information can be performed.

[0048] <Data write-in processing by user> drawing 8 is a flow chart which shows the data write-in actuation (henceforth "data write-in processing by the user") performed in a user phase. A user receives CD-R1 which finished above-mentioned "it having been information record processing at the time of shipment" in a commercial scene, sets the CD-R1 in the CD-R record regenerative apparatus 10, and starts processing of a graphic display.

[0049] Initiation of this processing publishes a write-in instruction from host equipment 21 first to the CD-R record regenerative apparatus 10. The CD-R record regenerative apparatus 10 answers this instruction, and reads ID information from the system area of CD-R1 (step S31), and it judges whether it is a support disk (step S32). A support disk is a disk made by a predetermined manufacturer or the predetermined manufacturer registered beforehand as above-mentioned. The CD-R record regenerative apparatus 10 holds ID information list (henceforth a "support list") of [for identifying these manufacturers], and at the above-mentioned step S32, with reference to the support list concerned, if ID information is registered, CD-R1 set in the CD-R record regenerative apparatus 10 will judge with it being a support disk.

[0050] the message (for example, -- " -- this disk is not a security response.) of the purport to which the exchange to a support disk is urged to host equipment 21 when the judgment result of step S32 is "no (NO)" (i.e., when CD-R1 set in the CD-R record regenerative apparatus 10 is not a support disk) Please exchange for the disk corresponding to security. The following processings are performed when the

judgment result of step S32 is "**" (YES) (i.e., when CD-R1 set in the CD-R record regenerative apparatus 10 is a support disk), while ") is sent out (step S33) and the write-in continuation or the write-in termination after disk-swapping is judged (step S38).

[0051] First, a secret flag is added to record data (step S34). This secret flag is data which are used as a check flag for forbidding reuse of the plaintext data after decode in a playback phase as above-mentioned, applied a technique like digital watermarking preferably, and secrecy-ized that existence. Subsequently, a cryptographic key is read from the system area of CD-R1 set in the CD-R record regenerative apparatus 10 (step S36), and after enciphering the record data which added the above-mentioned secret flag using the cryptographic key, the encryption data is recorded on the user area of CD-R1 (step S37).

[0052] When judging whether it writes in other CD-Rs1 finally (step S38) and continuing writing, while sending out a necessary message (for example, "set a new disk") to host equipment 21, when rejecting CD-R [finishing / writing]1, repeating step S31 or subsequent ones and not continuing writing, it writes in, CD-R1 of ending is rejected, and processing is ended.

[0053] Drawing 9 is drawing showing the time run of the above "data write-in processing by the user." In this drawing, while a user loads the CD-R record regenerative apparatus 10 with CD-R1, he operates host equipment 21 and publishes a necessary write-in instruction to the CD-R record regenerative apparatus 10. The CD-R record regenerative apparatus 10 answers this write-in instruction, ID information written in the system area of CD-R1 is read, and it collates with predetermined ID information list (support list), and judges whether it is a support disk. And if it is not a support disk, exchange of a disk will be urged to host equipment 21, and if it is a support disk, that will be notified to host equipment 21. Host equipment 21 answers advice of the purport which is a support disk, adds a secret flag to record data, and requires a cryptographic key from the CD-R record regenerative apparatus 10. The CD-R record regenerative apparatus 10 reads a cryptographic key from the system area of CD-R1, and transmits the cryptographic key to host equipment 21. Host equipment 21 enciphers record data (what added the secret flag) using the transmitted cryptographic key, the encryption data is transmitted to the CD-R record regenerative apparatus 10, and the CD-R record regenerative apparatus 10 records the transmitted encryption data on CD-R1.

[0054] Therefore, CD-R which has ID information indicated by the predetermined support list according to this "processing data write-in [by the user]", In short, only

about CD-R made by the specific manufacturer, to the user area Since the record data which added the secret flag can be enciphered and recorded, differentiation with CD-R made by the support list by the non-indicated manufacturer can be attained, and a predominance in a commercial scene can be acquired.

[0055] <Data regeneration by user> drawing 10 is the rough block block diagram of the playback special-purpose machine (henceforth a "CD-R regenerative apparatus") used for data playback of a user phase, and the difference with the above-mentioned CD-R record regenerative apparatus 10 (refer to drawing 6) is a point without the record function of data. Namely, this CD-R regenerative apparatus 30 (equivalent to the data regenerative apparatus for write-once mold optical disks given in the summary of invention) The spindle motor 32 which supports the clamping area of CD-R1 and carries out revolution actuation in the predetermined direction, The optical pickup 34 which spaces substrate 1b of CD-R1, and irradiates the laser 33 for playback at recording layer 1c, While having the coarse adjustment motor 35 made to move an optical pickup 34 to radial [of a disk] in harmony with the seeking motor which is not illustrated [which was prepared in the interior of an optical pickup 34] The disk roll control section 36 which controls the rotational speed of a spindle motor 32, The rotational speed of the coarse adjustment motor 35, and the coarse adjustment motor control section 37 which controls a hand of cut, It has the pickup control section 38 which performs control of the location of an optical pickup 34, or laser reinforcement, and the playback control section 39 which controls conversion of waveform of the reading signal from an optical pickup 34 etc., and has further the controller 40 which generalizes each of these control sections.

[0056] like the above-mentioned CD-R record regenerative apparatus 10, this CD-R regenerative apparatus 30 is built in the expansion slot of the host equipments 51, such as a personal computer, (or it carries out external -- having), connects between host equipment 51 and controllers 40 by cable 51a of predetermined signal specification (for example, SCSI), and is used.

[0057] The CD-R regenerative apparatus 30 which has such a configuration can reproduce information written in CD-R1 as it is shown below. in addition, CD-R1 -- CD-ROM -- although it is a compatible device and information playback of CD-ROM as well as the CD-R record regenerative apparatus 10 explained previously is possible for the CD-R regenerative apparatus 30, since there is no relation with direct this invention, explanation is omitted.

[0058] It has the structure where drawing 11 is the hierarchical functional conceptual diagram of host equipment 51, and as for the layered structure of a graphic display

make the lowest layer into the physical layer and it makes the top layer the application layer like the so-called OSI (Open System Interconnection: open systems interconnection) reference model. Driver layer 51b which roughly divides this structure and is closely related to the physical layer, Service layer 51c offered by the so-called operating system (OS) moreover located, It consists of 51d of the application layers for being located in the top layer and realizing a user interface. Application program (for example, thing containing user interface for using CD-R regenerative apparatus 30) 51e mounted in 51d of application layers Driver layer 51b is accessed through operating system 51f [of service layer 51c] API (Application Programmable Interface), for example, various resources including the CD-R regenerative apparatus 30 are used.

[0059] Here, various driver programs are mounted in driver layer 51b. For example, if interface specification of the CD-R regenerative apparatus 30 is set to SCSI, SCSI driver (it is also called ATAPI driver) 51g, IOS (Input/Output Supervisor) driver 51i miniport driver 51h for SCSI ports and for input/output control, etc. are mounted at least.

[0060] Although application program 51e generally uses the various resources located in the physical layer using operating system 51f predetermined API, he sees from application program 51e, and is not usually conscious of existence of these drivers. For example, when using the CD-R regenerative apparatus 30 from application program 51e, IOS driver 51i, SCSI driver 51g, and miniport driver 51h are used indirectly actually. Moreover, also when performing actuation of a file copy etc., IOS driver 51i is used indirectly actually.

[0061] By the way, special driver (henceforth "filter driver") 51j distinguished from others by hatching is mounted in driver layer 51b of a graphic display. This filter driver 51j is peculiar to this operation gestalt, and the monitor of the data passed to operating system 51f from the CD-R regenerative apparatus 30 according to the demand of (a) application program 51e at least is carried out. The first function to judge whether the above-mentioned "secret flag" is contained in the data, (b) When existence of the above "a secret flag" is judged, the copy actuation and preservation actuation of operating system 51f to the data concerned Refusal or a limit (For example, a copy instruction and a preservation instruction should be disregarded) It has the second function to carry out and is equivalent to a judgment means and a prohibition means given in the summary of invention.

[0062] In order to realize the first function, filter driver 51j is mounted between SCSI driver 51g and miniport driver 51h, and further, in order to realize the second function,

it is mounted between operating system 51f and IOS driver 51i. In addition, this mounting position is an example. What is necessary is to be the location which cannot be directly accessed from 51d of application layers in short, and to just be mounted in the location suitable for refusal of the above-mentioned monitor, the above-mentioned copy actuation, or preservation actuation. Moreover, filter driver 51j is not so single as a graphic display, and may be divided for every function.

[0063] A user accesses the CD-R regenerative apparatus 30, operating the user interface offered by application program 51e, and reproduces the data recorded on CD-R1. On the occasion of this regeneration, operating system 51f and the driver programs 51g-51j serve as a lentigo-intermediary, and do not appear in a table. That is, without being conscious of existence of operating system 51f and the driver programs 51g-51j, a user can access the CD-R regenerative apparatus 30, and can use the data recorded on CD-R1.

[0064] The data recorded on CD-R1 are seen from application program 51e, and are recognized as an independent meeting (file) of data managed by the file system of operating system 51c. A user can deal with it like the data in which this data was stored by other storage devices (file access). While the CD-R regenerative apparatus 30 reads the TOC information in a lead-in groove (RI) and provides driver layer 51b of host equipment 51 with it on the occasion of this file access When the read-out command of a specific file is received from the driver software layer 51b concerned While specifying the truck of a data area (UA) with which the data of the file concerned were written in with reference to the TOC information in a lead-in groove (RI) and locating an optical pickup 34 in the starting position of the truck The rotational speed of a spindle motor 32 is controlled, the laser 33 for playback is irradiated from an optical pickup 34 at CD-R1, the file data concerned is read, and a series of actuation of transmitting the reading data to driver layer 51b of host equipment 51 is performed.

[0065] Drawing 12 is a flow chart which shows the data playback actuation (henceforth "data regeneration by the user") performed in a user phase. CD-R1 in which encryption data (what added the secret flag to record data and was enciphered) were written by data write-in processing according [a user] to the above-mentioned user -- receiving -- the CD-R1 -- the CD-R regenerative apparatus 30 -- setting -- the CD-R1 to ID information -- reading (step S41) -- ID input is required from host equipment 51 (step S42). Host equipment 51 displays predetermined GUI (Graphical User Interface) of a purport which stimulates ID input on a screen, receives ID input from the keyboard by the user etc., and transmits inputted ID information to the CD-R

record regenerative apparatus 10. The CD-R regenerative apparatus 30 compares transmitted ID information with ID information read from CD-R1 (step S43), and when in agreement, while it judges it as a registered user and a user inaccurate when not in agreement and ends processing as it is at the time of decision of an inaccurate user, it performs the following processings at the time of decision of a registered user.

[0066] First, the cryptographic key and encryption data which are written in the system area of CD-R1 are read (step S44, step S45), and it transmits to host equipment 51. Host equipment 51 ends processing as it is, without performing decode actuation, when the secret flag is not contained while decoding the encryption data using a cryptographic key (step S47), returning to the data of a plaintext and presenting utilization of a user, when it is judged and (step S46) included whether the secret flag is contained in the transmitted data.

[0067] Drawing 13 is drawing showing the time run of the above "data regeneration by the user." In this drawing, while a user loads the CD-R regenerative apparatus 30 with CD-R1, he operates host equipment 51 and publishes a necessary playback instruction to the CD-R regenerative apparatus 30. The CD-R regenerative apparatus 30 answers this playback instruction, ID request is returned to host equipment 51, and host equipment 51 displays GUI of a purport which stimulates ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R1) according to the GUI, and host equipment 51 transmits inputted ID information to the CD-R regenerative apparatus 30.

[0068] The CD-R regenerative apparatus 30 reads ID information currently written in the system area of CD-R1, and coincidence with ID information transmitted from host equipment 51 is judged. If inharmonious, while judging it as an inaccurate user, stopping processing and refusing playback, if in agreement, it will be judged as a registered user, and the cryptographic key currently written in the system area of CD-R1 and the encryption data currently written in the data area are read, and it transmits to host equipment 51. Host equipment 51 ends processing, without performing decode actuation, when the secret flag is not contained while encryption data are decoded using the cryptographic key and access from a registered user is permitted, when it judges whether there is any secret flag and the secret flag is contained in transfer data.

[0069] Therefore, when according to this "data regeneration by the user" a registered user and an inaccurate user can be identified using ID information currently written in the system area of CD-R and data regeneration is performed by the registered user, the cryptographic key written in the system area of CD-R and the encryption data

written in the data area can be transmitted to host equipment. And when the secret flag is contained in transfer data, encryption data can be decoded with host equipment and accesses (for example, access thru/or activation, etc. of data) to the decoded raw data can be permitted in the registered user concerned.

[0070] Consequently, while being able to eliminate an inaccurate user and being able to reproduce data Since only decode of the encryption data with which the secret flag is contained can be performed, with combination with the aforementioned "data write-in processing by the user" In a series of security countermeasures from a record phase to a playback phase being establishable, the activity of the support disk made by the specific manufacturer as a record medium indispensable to these security countermeasures can be forced.

[0071] <Disk copy processing by user> drawing 14 is a flow chart which shows the data copy actuation (henceforth "data copy processing by the user") performed in a user phase. In addition, although the copy-of-data point is made into CD-R in the following explanation, this may be an example of data reuse and a copy place may be what kind of storage. You may be a hard disk and other record media.

[0072] In drawing 14 , if the data copy processing by the user is started, by data write-in processing by the above-mentioned user, a user will make non-recorded CD-R a copy place copy-CD-R1 in which encryption data (what added secret flag to record data and was enciphered) were written origin, and will set each in the CD-R regenerative apparatus 30 of a copied material, and the CD-R record regenerative apparatus 10 of a copy place. And host equipment 51 is operated and a copy instruction is published to the CD-R regenerative apparatus 30 of a copied material. ID input is required from host equipment 51 the CD-R regenerative apparatus 30 of a copied material answering a copy instruction, and beginning (step S51) to read ID information from CD-R1 (step S52). Host equipment 51 displays predetermined GUI of a purport which stimulates ID input on a screen, receives ID input from the keyboard by the user etc., and transmits inputted ID information to the CD-R regenerative apparatus 30 of a copied material.

[0073] The CD-R regenerative apparatus 30 of a copied material compares transmitted ID information with ID information read from CD-R1 (step S53). When in agreement, while judging it as a registered user, judging it as an inaccurate user when not in agreement and ending processing as it is at the time of decision of an inaccurate user, at the time of decision of a registered user The cryptographic key and encryption data which are written in the system area of CD-R1 of a copied material are read, and it transmits to host equipment 51. Host equipment 51 by filter

driver 51j mounted in the driver layer 51b If it judges whether a secret flag exists (step S54) and a secret flag does not exist in transfer data While decode encryption data using the transmitted cryptographic key, the decode data is transmitted to the CD-R record regenerative apparatus 10 of a copy place, copy processing in which it records on CD-R1 of a copy place is performed (step S55) and processing is ended If the secret flag exists, this copy processing will be stopped compulsorily (step S56), and processing will be ended.

[0074] Drawing 15 is drawing showing the time run of the above "data copy processing by the user", and the thing of a copied material, the CD-R record regenerative apparatus 10, and CD-R1' of CD-R1 and the CD-R regenerative apparatus 30 in drawing are the things of a copy place. In this drawing, while a user loads the CD-R regenerative apparatus 30 and the CD-R record regenerative apparatus 10 with CD-R1 of a copy place, and 1' a copied material, respectively, he operates host equipment 51 and publishes a necessary copy instruction to the CD-R regenerative apparatus 30 of a copied material. The CD-R regenerative apparatus 30 of a copied material answers this copy instruction, ID request is returned to host equipment 51, and host equipment 51 displays GUI of a purport which stimulates ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R1) according to the GUI, and host equipment 51 transmits inputted ID information to the CD-R regenerative apparatus 30 of a copied material.

[0075] the CD-R regenerative apparatus 30 of a copied material carries out the reading appearance of the ID information currently written in the system area of CD-R1, judges coincidence with the ID information transmitted from host equipment 51, if it is inharmonious, while it judges to be an inaccurate user and will end processing, if it is in agreement, it will judge to be a registered user, carries out the reading appearance of the cryptographic key and the encryption data currently written in CD-R1, and transmits them to host equipment 51. Host equipment 51 judges existence of the secret flag in transfer data by filter driver 51j mounted in the driver layer 51b. And if it does not exist while stopping copy processing compulsorily, if it exists, encryption data are decoded using a cryptographic key, the decode data is transmitted to the CD-R record regenerative apparatus 10 of a copy place, and the CD-R record playback measure 10 of a copy place writes the transfer data in CD-R1'.

[0076] Therefore, even if it is a registered user, that copy actuation is stopped compulsorily (refusal of copy actuation), and it can avoid performing it, when the copy of data to which the secret flag was added tends to be performed, while a registered user and an inaccurate user are discriminable using ID information currently written in

the system area of CD-R of a copied material according to this "data copy processing by the user." Consequently, when a secret flag exists in encryption data, since copy processing can be forbidden positively, reuse of decode data can be prevented and security can be given covering all the phases from record to playback.

[0077] According to the gestalt of this operation, it can judge whether it is a manufacturer's CD-R1 (support disk) indicated by the support list using ID information written in the system area of CD-R1, the record data which added the secret predetermined flag in the case of the support disk can be enciphered, and it can record on CD-R1 as explained more than the <conclusion>. And it is a playback side, and in case this encryption data is read, the existence of a secret flag is inspected, and when there is a secret flag, reuse of decode data can be forbidden. Therefore, since only the decode data temporarily made by the above-mentioned "data regeneration by the user" on main memory exist in the interior of host equipment 51, And it is this temporary data at the completion event of utilization from a process, and since it is released promptly, the trace of reusable decode data is not left behind and the exceptional useful effectiveness that unjust runoff of data etc. can be prevented certainly is acquired.

[0078] in addition, in the above explanation, although hiding information, such as ID information and a cryptographic key, is written in the system area, this system area may be the semantics of fields other than the field (typically data area) where direct access by the user was permitted, and you may be a lead-in groove not to mention above-mentioned PCA and PMA, and may be lead-out, or fields other than this exist -- you may be that field as long as it becomes.

[0079] Moreover, although explanation was not added especially about a cryptographic key, any of various cipher systems (for example, there are methods, such as FEAL:Fast Encipherment Algorithm, besides the above-mentioned DES method.) which are generally known may be adopted. What is necessary is to take into consideration the difficulty of decode, the overhead of encryption processing or decode processing, the volume of encryption data, etc., and just to adopt a suitable method.

[0080] Moreover, the function to forbid especially reuse of decode data among the security functions of said explanation Although organic association with software resources, such as filter driver 51j chiefly mounted in host equipment 51, and other general-purpose drivers, an operating system, and the various hardware resources of host equipment 51 realizes functionally Since resources other than filter driver 51j can use a general-purpose thing, being together put by the program of filter driver 51j

can say substantially an indispensable matter indispensable for "the function to forbid reuse of decode data" of said explanation. Therefore, the point of the security function concerning this invention includes the component (a unit article, a finished product, or semifinished product) containing record media or these record media, such as the floppy disk and optical disk which stored all those programs or its important section, a compact disk, a magnetic tape, a hard disk, or semiconductor memory. In addition, what the record medium or component has on a network not to mention that by which itself is in a distribution channel, and offers only the content of record is contained.

[0081] Moreover, in the above explanation, although the example of CD-R was shown as a write-once mold optical disk, it does not restrict to this. For example, since DVD(Digital Video Disc or Digital Versatile Disc)-R can also perform one data writing, of course, he is the associate of a write-once mold optical disk. What is necessary is to read a CD-R record regenerative apparatus and a CD-R writer with a DVD-R record regenerative apparatus and a DVD-R writer, respectively, and just to replace them, while reading CD-R as DVD-R, when applying the above-mentioned explanation to DVD-R.

[0082]

[Effect of the Invention] According to invention according to claim 1, if a secret predetermined flag is detected at the time of playback of data, generation of the duplicate object of playback data will be restricted. Therefore, reuse of playback data can be prevented and the security in a playback phase can be secured. According to invention according to claim 2, based on the security information stored in the state of invisibility, access to an optical disk is restricted to the system area of an optical disk. It follows, for example, a valid user can be attested and written in at the time of data playback, access to data can be permitted, and an inaccurate user's abatement etc. can aim at improvement in security nature. According to invention according to claim 3, if a secret predetermined flag is detected at the time of playback of data, generation of the duplicate object of playback data will be forbidden. Therefore, reuse of playback data can be prevented and the security in a playback phase can be secured. According to invention according to claim 4, said judgment means and a prohibition means are realizable with organic association with the hardware resource and this program containing a microcomputer.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the utilization mimetic diagram of CD-R of this operation gestalt.
[Drawing 2] It is the external view and its important section enlarged drawing of a write-once mold optical disk.
[Drawing 3] It is cross-section structural drawing of CD-R.
[Drawing 4] It is the format conceptual diagram of each record section of CD-R.
[Drawing 5] It is instantiation structural drawing of the data format containing ID information written in the system area of CD-R, and a cryptographic key.
[Drawing 6] It is the rough block block diagram of a CD-R record regenerative apparatus.
[Drawing 7] It is the flow chart which shows information record processing at the time of shipment.
[Drawing 8] It is the flow chart which shows the data write-in processing by the user.
[Drawing 9] It is drawing showing the time run of the data write-in processing by the user.
[Drawing 10] It is the rough block block diagram of a CD-R regenerative apparatus.
[Drawing 11] It is the hierarchical functional conceptual diagram of host equipment.
[Drawing 12] It is the flow chart which shows the data regeneration by the user.
[Drawing 13] It is drawing showing the time run of the data regeneration by the user.
[Drawing 14] It is the flow chart which shows the disk copy processing by the user.
[Drawing 15] It is drawing showing the time run of the disk copy processing by the user.
[Drawing 16] It is the conceptual diagram of the conventional security countermeasures.
[Description of Notations]

PCA Power Calibration Area (system area)
1 CD-R (Write-once Mold Optical Disk)
30 CD-R Regenerative Apparatus (Data Regenerative Apparatus for Write-once Mold Optical Disks)
51j Filter driver (a judgment means, prohibition means)

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－332019
（P2001－332019A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数４　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－144456(P2000－144456)

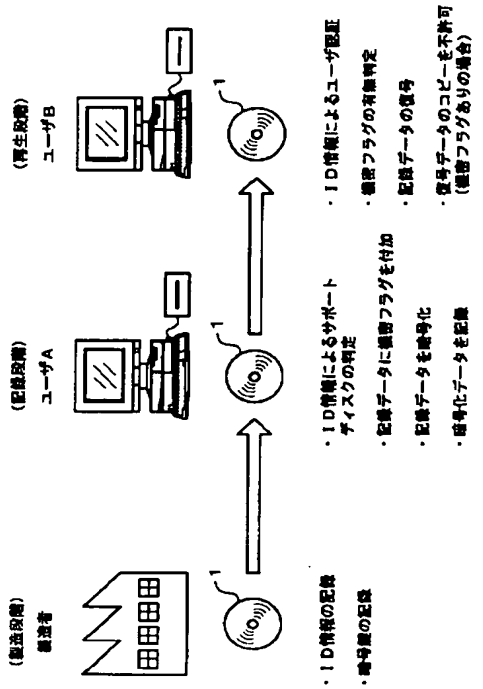
(22)出願日　平成12年５月17日(2000.5.17)

(71)出願人　000204284
太陽誘電株式会社
東京都台東区上野６丁目16番20号
(72)発明者　大村　幸秀
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(72)発明者　砂川　隆一
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(74)代理人　100096699
弁理士　鹿嶋　英實

最終頁に続く

(54)【発明の名称】　ライトワンス型光ディスク用データ記録再生方法、ライトワンス型光ディスク用データ再生装置および記録媒体

(57)【要約】
【課題】　再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスク用データ記録再生技術を提供する。
【解決手段】　ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込み、前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する。再生データの再利用を阻止し、再生段階におけるセキュリティを確保できる。



1

【特許請求の範囲】

【請求項１】　ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込む書き込み工程と、

前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する複製制限工程と、

を含むことを特徴とするライトワンス型光ディスク用データ記録再生方法。

【請求項２】　前記光ディスクのシステム領域に格納されたセキュリティ情報に基づき該光ディスクへのアクセスを制限するアクセス制限工程をさらに具備することを特徴とする請求項１記載のライトワンス型光ディスク用データ記録再生方法。

【請求項３】　ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を備えたことを特徴とするライトワンス型光ディスク用データ再生装置。

【請求項４】　ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、

該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、

を実現するためのプログラムを格納したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ライトワンス型光ディスク用データ記録再生方法、データ再生装置および記録媒体に関する。詳しくは、１回だけデータを書き込むことができるＣＤ－Ｒ（Compact Disc Recordable）に代表されるライトワンス型光ディスクに適用するデータ記録再生方法、データ再生装置および記録媒体に関する。

【０００２】

【従来の技術】各種コンテンツやコンピュータプログラム等の電子データの配布媒体に、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）が多用されている。ＣＤ－ＲＯＭは、電子データを記録したマスタＣＤからプレス成型等によって製造される複製物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版ＣＤやプライベートＣＤなどには、データの消去や上書きができない（追記は可能）ライトワンス型の光ディスク装置、典型的にはＣＤ－Ｒが用いられる。

2

ＣＤ－Ｒは透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点でＣＤ－ＲＯＭと構造上の違いがあり、専用の記録装置（ＣＤ－Ｒライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ピットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【０００３】ＣＤ－Ｒは、上記のとおりデータの消去や上書きができないライトワンス型の記録媒体である。すなわち、一度書き込んだデータの消去や書き換えが不可能である。そのため、不正者によるデータの消去や改ざんを確実に防止できるという優れた利点を持つことから、今日、特に秘匿を要する電子データの保管や配布などの用途に欠かせない記録媒体としての地位を確立しているが、反面、ＣＤ－Ｒは記録情報の読み出しが自由であるが故に、情報の不正読み出しや不正コピーを防止できないという欠点も持っている。

【０００４】そこで、秘匿を要するデータを記録する際に、例えば、図１６に示すように、暗号化して記録することが行われている。図において、平文データ１００は暗号化前の“生”のデータであり、例えば、可読性を有するテキスト形式のデータである。この平文データ１００を不可視化して記録する場合、まず、所定の暗号化ツール１０１を用いて暗号化データ１０２に変換する。暗号化の方式は特に限定しないが、暗号鍵と復号鍵に共通の鍵を用いる共通鍵方式である。以下、この鍵のことを代表して「暗号鍵」ということにする。したがって、以下において、暗号鍵という場合は復号鍵も意味することとする。

【０００５】さて、暗号化されたデータ（図においては暗号化データ１０２）は不可視データであり、そのまま配布しても安全（計算量的に安全）であるため、この暗号化データ１０２をＣＤ－Ｒ１０３に書き込むことによってデータの不正読み取りを防止し、セキュリティを保つことができる。再生の際は、ＣＤ－Ｒ１から暗号化データ１０４を読み出し、所定の復号ツール１０５を用いて平文データ１０６に戻せば（復号すれば）よい。

【０００６】

【発明が解決しようとする課題】しかしながら、上記のセキュリティ対策にあっては、復号後のデータ（平文データ１０６）の再利用が自由であり、データ保全の効果はもっぱらＣＤ－Ｒ１０３に収められた状態でしか得られないという不都合がある。すなわち、ＣＤ－Ｒ１０３から読み出されて復号された後の平文データ１０６については、まったくセキュリティがかかっておらず、この平文データ１０６に対するデータ保全は単に再生側ユーザのモラルに期待するしかないという問題点があった。

【０００７】したがって、本発明が解決しようとする課題は、再生側ユーザのモラルに期待することなく復号後の平文データの再利用を確実に禁止し、以って、記録か

ら再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスク用データ記録再生技術を提供することにある。

【０００８】

【課題を解決するための手段】請求項１記載のライトワンス型光ディスク用データ記録再生方法は、ライトワンス型光ディスクにデータを書き込む際に所定の機密フラグを前記データに付加して書き込む書き込み工程と、前記書き込みデータを再生する際に前記機密フラグの有無を検査して機密フラグの存在が検出された場合に前記データの複製物の生成に関する動作を制限する複製制限工程と、を含むことを特徴とする。これによれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が制限される。請求項２記載のライトワンス型光ディスク用データ記録再生方法は、請求項１記載のライトワンス型光ディスク用データ記録再生方法において、前記光ディスクのシステム領域に格納されたセキュリティ情報に基づき該光ディスクへのアクセスを制限するアクセス制限工程をさらに具備することを特徴とする。これによれば、光ディスクのシステム領域に不可視状態で格納されたセキュリティ情報に基づいて光ディスクへのアクセスが制限される。請求項３記載のライトワンス型光ディスク用データ再生装置は、ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、を備えたことを特徴とする。これによれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が禁止される。請求項４記載の記録媒体は、ライトワンス型光ディスクから読み込まれたデータの中に所定の機密フラグが含まれているか否かを判定する判定手段と、該判定手段によって機密フラグの存在が判定された場合に前記データの複製物の生成に関する動作を禁止する禁止手段と、を実現するためのプログラムを格納したことを特徴とする。これによれば、マイクロコンピュータを含むハードウェアリソースと該プログラムとの有機的結合によって前記判定手段および禁止手段が実現される。

【０００９】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、以下の説明における様々な細部の特定ないし実例および数値や文字列その他の記号の例示は、本発明の思想を明瞭にするための、あくまでも参考であって、それらのすべてまたは一部によって本発明の思想が限定されないことは明らかである。また、周知の手法、周知の手順、周知のアーキテクチャおよび周知の回路構成等（以下「周知事項」）についてはその細部にわたる説明を避けるが、これも説明を簡潔にするためであって、これら周知事項のすべてまたは一部を意図的に排除するものではない。かかる周知事項は本発明の出願時点で当業者の知り得るところであるので、以下の説明に当然含まれている。

【００１０】まず、本実施形態のライトワンス型光ディスク（以下「ＣＤ－Ｒ」という。）の利用形態を大まかに説明する。図１は、本実施形態のＣＤ－Ｒ１の利用模式図である。この図では、製造者（メーカ）によるＣＤ－Ｒ１の製造段階、ユーザＡによる当該ＣＤ－Ｒ１への秘匿を要するデータの記録段階、および、ユーザＢによる当該記録済みＣＤ－Ｒ１からデータを読み出して再生する再生段階の三つの段階が示されている。

【００１１】後の説明からも明らかになるが、（１）製造段階ではＣＤ－Ｒ１に固有の識別情報（以下「ＩＤ情報」という。）と所定の暗号化方式における暗号鍵（復号鍵を兼ねるもの）とをＣＤ－Ｒ１に電子的に記録して出荷する。ＩＤ情報と暗号鍵の記録場所はユーザからの直接的なアクセスが許可されていない場所（システム領域；領域構造については後述する。）である。（２）記録段階ではそのＣＤ－Ｒ１のＩＤ情報から当該ＣＤ－Ｒ１が所定の製造者またはあらかじめ登録された製造者によって作られたもの（以下「サポートディスク」という。）であるか否かを判定し、サポートディスクである場合に、記録データに所定の“機密フラグ”を付加すると共に、ＣＤ－Ｒ１に書き込まれている暗号鍵を用いて記録データ（機密フラグを付加したもの）を暗号化し、その暗号化データをＣＤ－Ｒ１に記録する。（３）再生段階ではＣＤ－Ｒ１のＩＤ情報を用いてユーザ認証を行い、正規ユーザ（ＩＤ情報を知っているユーザ）に対してのみ暗号化データの復号処理を許容すると共に、復号データのコピーや保存等の複製処理を実行して再利用を行う場合は、記録データ中の“機密フラグ”の有無を判定し、機密フラグ有りの場合は上記再利用を拒否、例えば、コピー動作や保存動作を強制中断する。

【００１２】これら三つの段階において、ＣＤ－Ｒ１にセキュリティを持たせるための工夫は、❶製造時にＣＤ－Ｒ１のシステム領域にＩＤ情報と暗号鍵を書き込むようにしたこと、❷ユーザＡによる記録時に、記録データに“機密フラグ”を付加するようにしたこと、❸同記録時に記録データ（機密フラグ付）を暗号化してＣＤ－Ｒ１に書き込むようにしたこと、❹ユーザＢによる再生時にＩＤ情報によるユーザ認証を行って正規ユーザに対してのみ暗号化データの復号を許可するようにしたこと、❺同再生時に復号データの再利用が行われる場合は機密フラグの有無を判定して機密フラグ有りの場合にその再利用動作を強制中断するようにしたことにある。

【００１３】❶のＩＤ情報はデータ再生時のユーザ認証に用いられ、また、❶の暗号鍵はデータの暗号化と正規ユーザによって行われる暗号化データの復号に用いられる。これらのＩＤ情報と暗号鍵はＣＤ－Ｒ１の記録領域のうちユーザアクセスが許可されていない領域（システ

ム領域）に書き込まれた、いわば不可視化された“隠しデータ”である。❶のＩＤ情報はまたデータ書き込み時におけるサポートディスクの判定にも用いられる。サポートディスクとは、前記のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたＣＤ－Ｒ１のことであり、正確には“機密フラグ”を用いて行われる復号後データの再利用禁止対策を“サポート”した特別なディスク（ＣＤ－Ｒ１）であることを意味する。

【００１４】ここで、機密フラグはその名前のとおりフラグ形式のデータであってもよいし、フラグ以外の別形式であってもよい。留意すべき点は機密フラグ（または機密フラグと同等のもの）の存在がユーザに対して秘匿化されていなければならないことにある。一般にフラグ形式のデータは二値論理（ブーリアン型ともいう。）の１ビットデータであり、そのビット位置を非公開とすることによって一応の秘匿化は可能であるが、総当りで調べられた場合にフラグの位置が見破られるおそれを否定できないため、望ましくは、電子透かしのような積極的な秘匿化対策を講じたデータとすることが好ましい。電子透かしとは、オリジナルデータの品質を損なうことなく、そのオリジナルデータの周波数、空間または時間の一つまたは複数のドメインに所定のメッセージ情報を隠す（埋め込む）ことをいう。機密フラグは、再生段階において、復号後の平文データの再利用（平文データを他の記録媒体にコピーや保存したりすること；複製動作ともいう。）を禁止するためのチェックフラグとして用いられる。これにより、暗号化データによるＣＤ－Ｒ１のセキュリティに加え、復号後の平文データのセキュリティ対策も講じることができ、本願発明の課題である、再生側ユーザのモラルに依存することなく復号後の平文データの再利用を禁止でき、以って、記録から再生までのあらゆる段階のセキュリティを確保できるライトワンス型光ディスクを提供することができるのである。

【００１５】以下、上記課題達成に必要な構成および作用について、具体例をあげて説明する。図２は、本実施形態におけるＣＤ－Ｒ１の外観図（ａ）およびその要部拡大図（ｂ）である。これらの図において、ＣＤ－Ｒ１は、直径１２ｃｍ（直径８ｃｍのものもある。以下、直径１２ｃｍのもので説明する。）のディスク状を有しており、ディスクの中心に直径１５ｍｍのセンターホール１ａが形成されている。ディスクの中心Ｔ０からセンタホール１ａの壁（ディスク内縁Ｔ１）までの距離は７．５ｍｍ、Ｔ０からディスク外縁Ｔ７までの距離は６０ｍｍであり、このＴ１～Ｔ７の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にＰＣＡ（Power Calibration Area）、ＰＭＡ（Program Memory Area）、リードイン（図では「ＲＩ」と略している。）、データエリア（図では「ＵＡ」と略している。）およびリードアウト（図では「ＲＯ」と略している。）の各領域が設けられている。

【００１６】各領域を概説すると、Ｔ２～Ｔ３に位置するＰＣＡは、ＣＤ－Ｒ１にデータを記録する際に行われるレーザ強度調整のための試し書き領域である。この試し書きは一般に１００回程度可能であり、少なくとも１回のデータ記録で１回分の領域を消費する。Ｔ３～Ｔ４に位置するＰＭＡは、ＣＤ－Ｒ１でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始／終了位置を一時的に保存する領域である。Ｔ４～Ｔ５に位置するリードイン（ＲＩ）は、セッショントラックの先頭（ディスクの内周側）にある領域で、セッションのＴＯＣ（Table OfContents：ＣＤに記録されているトラック数、開始位置およびデータ領域の合計の長さ）を保存する領域である。セッションをクローズすると、ＰＭＡに一時保存されていた情報がこのリードイン（ＲＩ）に書き込まれる。

【００１７】Ｔ５～Ｔ６に位置するデータエリア（ＵＡ）は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約６８０Ｍバイト（直径８ｃｍのものは最大約１９０Ｍバイト）であり、この記憶容量は録音時間で表すと最大約７４分（直径８ｃｍのものは最大約２１分）になる。データエリア（ＵＡ）は、リードイン（ＲＩ）のすぐ後ろから連続する所定サイズ（２Ｋバイト）単位の論理ブロックで管理されるようになっており、各論理ブロックごとに０から最大約３００００までのＬＢＮ（Logical Block Number）が割り当てられるようになっている。Ｔ６～Ｔ７に位置するリードアウト（ＲＯ）は、セッションの最後（ディスクの外周側）にある領域で、データエリア（ＵＡ）の最後に到達したことを示す領域である。

【００１８】これら各領域のディスク上の位置はＴ３を除いて規格化されている。すなわち、Ｔ２はＴ０から２２．５ｍｍ離れた位置、Ｔ４はＴ０から２３ｍｍ離れた位置、Ｔ５はＴ０から２５ｍｍ離れた位置、Ｔ６はＴ０から５８ｍｍ離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト（ＲＯ）の終了位置とを同一の符号（Ｔ７）で示しているが、これは図示の都合である。リードアウト（ＲＯ）の実際の終了位置はＴ０から５８．５ｍｍ離れた位置になる。以下、特に断りのない限り、Ｔ７はリードアウト（ＲＯ）の終了位置を表すものとする。ちなみに、リードアウト（ＲＯ）の開始と終了位置（Ｔ６およびＴ７）はＣＤ－Ｒ１に記録するデータの量に応じて変化する。上記の実際値（Ｔ６＝５８ｍｍ、Ｔ７＝５８．５ｍｍ）は記憶データ量を最大にしたときのものである。

【００１９】図３は、ＣＤ－Ｒ１の断面構造図である。ＣＤ－Ｒ１は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性（屈折率や複屈折など）を備えた材料（例えばプラスチック）からなる基板１ｂの上に、有機色素からなる記録層１ｃ、アルミニウムなどの金属材料からなる反射層１ｄおよび樹脂等の硬質材料

からなる保護層１ｅを積層して形成されている。断面全体の厚さは１．２ｍｍである。

【００２０】ＣＤ－ＲＯＭとの構造上の相違は、記録層１ｃを有する点、および記録層１ｃと基板１ｂとの間にウォッブルグルーブと呼ばれる渦巻状の案内溝１ｆが形成されている点にある。ＣＤ－Ｒ１へのデータの記録は基板１ｂの裏側から案内溝１ｆに沿って記録用の強いレーザを照射し、記録層１ｃを加熱して情報ピット（Ｐｉｔ：再生用のレーザ反射光を変調するための物理的変形変質部分）を形成することにより行われる。案内溝１ｆは、ディスクの内周側から外周側（または外周側から内周側）に向かって一筆書きの要領で連続して形成されており、案内溝１ｆの幅は約０．５～０．７μｍ、間隔は約１．６μｍである。ユーザ段階におけるデータ記録は、案内溝１ｆに沿って、その案内溝１ｆ（または案内溝１ｆの間のランド部）直下の記録層１ｃに情報ピットを形成することによって行われる。なお、ＣＤ－Ｒ１の裏側から見て案内溝１ｆの凸部分をランド（山）、凹部分をグルーブ（谷）といい、一般に谷の部分をウォッブルグルーブというが、本明細書では山と谷を区別しない。

【００２１】ここで、案内溝１ｆの一の役割は、ユーザ段階のデータ記録時にディスクの回転速度を制御するためのタイミング情報を保持することにある。この役割のため、案内溝１ｆは、所定の周期（例えば２２．０５ｋＨｚに相当する周期）で蛇行（「ウォブリング」ともいう。）する形状に形成されている。データの記録時には、この蛇行を光ピックアップでトレースして周期を検出し、その検出周期が一定となるようにディスクの回転速度を制御することにより、データ記録時の光ピックアップとディスク間の相対速度を一定に保つ。案内溝１ｆの他の役割は、ディスク上の各記録領域（ＰＣＡ、ＰＭＡ、ＲＩ、ＵＡおよびＲＯ）の位置情報をはじめとした様々なディスク情報を保持することにある。ディスク情報はＡＴＩＰ（Absolute Time In Pregroove：通称「Ａチップ」という。）とも呼ばれており、ＡＴＩＰには、上記の位置情報のほかに、基準の記録レーザ強度やディスク回転速度、アプリケーションコードあるいはディスクタイプなどの各種情報が含まれている。

【００２２】図４は、ＣＤ－Ｒ１の各記録領域のフォーマット概念図である。この図において、ＰＣＡ、ＰＭＡ、リードイン（ＲＩ）、データエリア（ＵＡ）およびリードアウト（ＲＯ）はそれぞれ、図２（ｂ）における同名部分に対応する。ＰＣＡおよびＰＭＡのサイズ（情報書き込み可能容量）は特に決められていないが、前述の試し書き回数（一般に１００回程度）やセッション情報の一時記憶回数に見合った必要量、例えば、ＰＣＡで約３．５Ｍバイト程度、ＰＭＡで約２Ｍバイト程度の容量が確保されている。ちなみに、これらの例示容量からＰＣＡの開始位置（Ｔ２）とＰＭＡの開始位置（Ｔ３）は、規格化されたリードイン（ＲＩ）の開始位置（Ｔ４）を基準として、「Ｔ２＝Ｔ４－約３５秒」の位置、「Ｔ３＝Ｔ４－約１３秒」の位置と書き表すことができる。

【００２３】既述のとおり、ＰＣＡはデータ記録を行う際の試し書き領域、ＰＭＡはクローズされていないセッション情報を一時的に格納する領域であるから、これら二つの領域（ＰＣＡ／ＰＭＡ）はデータ記録時にのみ利用（アクセス）される領域である。一方、リードイン（ＲＩ）はクローズされたセッション情報をＴＯＣとして記録する領域、データエリア（ＵＡ）は実際にデータが書き込まれる領域、リードアウト（ＲＯ）はデータエリアの終わりを明示する領域であるから、これら三つの領域（リードイン／データエリア／リードアウト）はデータ記録時と再生時の両方で利用（アクセス）される領域である。

【００２４】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、ＣＤ－Ｒ１の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール（典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど）を用いて容易にアクセスできるか否かの点で評価すると、データエリア（ＵＡ）については当然ながらその記憶内容の全容把握は可能であるが、他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）の内容把握は不可能である。

【００２５】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるため、かかる例外的なツールの利用を除けば、データエリア以外の他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）は、システムからのアクセスだけが許可された特殊な領域であるということができる。本明細書では、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」という。すなわち、データエリア（ＵＡ）はユーザ領域、それ以外のＰＣＡ、ＰＭＡ、リードイン（ＲＩ）およびリードアウト（ＲＯ）はシステム領域である。

【００２６】本実施の形態におけるＣＤ－Ｒ１は、先に説明したとおり、製造段階でシステム領域の一部にＣＤ－Ｒ１の固有情報（以下「ＩＤ情報」という。）と所定の暗号鍵情報とが書き込まれる。ＩＤ情報はＣＤ－Ｒ１の全製造数にわたってユニークな値（重複しない値）を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。

【００２７】このＩＤ情報は、後述するように、ユーザ段階でのＣＤ－Ｒ１へのアクセス照合に用いられる。例

えば、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（ＩＤを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【００２８】ＣＤ－Ｒ１に書き込まれたＩＤ情報のユーザへの通知は、各々のＣＤ－Ｒ１の購入者（または正規入手者）ごとに行わなければならない。例えば、あるＣＤ－Ｒ１（以下、便宜的に「ディスクＡ」とする。）に書き込まれたＩＤ情報を“ａｂｃｄｅｆ”と仮定すると、ディスクＡの購入者または正規入手者に対し、当該ＩＤ情報（“ａｂｃｄｅｆ”）を書面ないしその他の手段で通知する。この手段としては、例えば、ディスクＡのパッケージ（ディスクＡを収めたプラスチックケース）の中に当該ＩＤ情報（“ａｂｃｄｅｆ”）を記載した紙片を入れておいてもよいし、ディスクＡの購入時等に口頭で伝えてもよい。その他いろいろな手段が考えられるが、要は、出荷時にＣＤ－Ｒ１に書き込んだＩＤ情報をユーザに正確に伝達できればよい。

【００２９】一方、製造段階でシステム領域に一緒に書き込まれる鍵情報は、ユーザ段階でデータエリアに書き込まれる生データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをＣＤ－Ｒ１のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【００３０】したがって、ＩＤを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【００３１】図５は、システム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。この図において、第一の例（ａ）は、８バイトのＩＤ情報、８バイトのＤＥＳ（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で２０バイトの大きさを有している。また、第二の例（ｂ）は、８バイトのＩＤ情報、２４バイトのトリプルＤＥＳ暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で３６バイトの大きさを有している。いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構造はあくまでも例示である。要はＣＤ－Ｒ１の固体識別が可能な情報（ＩＤ情報）と、生データを暗号化データに変換できる共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とをＣＤ－Ｒ１のシステム領域に書き込んでおけばよい。

【００３２】図６は、ライトワンス型光ディスク記録再生装置（以下「ＣＤ－Ｒ記録再生装置」という。）の概略的なブロック構成図である。このＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１のクランピングエリア（図２（ａ）のＴ１～Ｔ２の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ１２と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに記録用または再生用のレーザ（一般に波長７７０～８３０ｎｍの赤外レーザ）１３を照射する光ピックアップ１４と、光ピックアップ１４の内部に設けられた不図示のシークモータと協調して光ピックアップ１４をディスクの半径方向に移動させる粗動モータ１５とを備えると共に、スピンドルモータ１２の回転速度を制御するディスク回転制御部１６と、粗動モータ１５の回転速度と回転方向を制御する粗動モータ制御部１７と、光ピックアップ１４の位置やレーザ強度の制御を行うピックアップ制御部１８と、光ピックアップ１４からの読み取り信号や光ピックアップ１４への書き込み信号の波形変換等の制御を行う再生／記録制御部１９とを備え、さらに、これらの各制御部を統括するコントローラ２０を備える。

【００３３】ＣＤ－Ｒ記録再生装置１０は、パーソナルコンピュータ等のホスト装置２１の拡張スロットに内蔵され（または外付けされ）、ホスト装置２１とコントローラ２０との間を所定の信号規格（例えば、ＳＣＳＩ：Small Computer System Interface）のケーブル２１ａで接続して用いられる。

【００３４】このような構成を有するＣＤ－Ｒ記録再生装置１０は、以下に示すとおり、ＣＤ－Ｒ１への情報の記録とその記録情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ記録再生装置１０は、ＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００３５】＜ＣＤ－Ｒ１への情報の記録動作＞ホスト装置２１でＣＤ－Ｒ記録専用アプリケーションプログラム（以下「ライティングプログラム」という。）を実行すると、まず、ライティングプログラムからのレーザ強度キャリブレーションコマンドがコントローラ２０に伝

えられる。コントローラ２０はこのコマンドに応答して各制御部に所要の指令を伝え、光ピックアップ１４をＣＤ－Ｒ１のＰＣＡ空領域（試し書きされていない領域）に位置させると共に、スピンドルモータ１２の回転速度を制御（光ピックアップ１４の現在位置における相対速度が所定速度となるように制御）した後、光ピックアップ１４から暫定強度（５．５～８ｍＷの間の任意パワー）の記録用レーザ１３をＰＣＡ空領域に照射して試し書きを行う。光ピックアップ１４の位置制御およびスピンドルモータ１２の回転速度制御は、ＣＤ－Ｒ１の案内溝１ｆのトレース信号から再生された情報（タイミング情報およびＡＴＩＰ情報）に従って行われる。

【００３６】次いで、コントローラ２０は、再生／記録制御部１９を介してＰＣＡに試し書きされたデータを読み取り、そのデータをホスト装置２１のライティングプログラムに返送する。ライティングプログラムは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が“否”であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が“適”であれば、ＣＤ－Ｒ１への情報の記録動作を開始する。

【００３７】この記録動作は、ユーザによって適宜に選択された所要の記録データをライティングプログラムからコントローラ２０に伝え、このコントローラ２０の制御の下、各制御部を介してスピンドルモータ１２の回転制御および光ピックアップ１４の位置制御を行いつつ、上記記録データで光ピックアップ１４からの記録用レーザ１３を変調しながらＣＤ－Ｒ１のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のＴＯＣをリードイン（ＲＩ）に書き込むと共に、最終セッションの後にリードアウト（ＲＯ）を形成する。

【００３８】＜ＣＤ－Ｒ１の記録情報の再生動作＞ＣＤ－Ｒ１の記録情報を再生する際に上記ライティングプログラムは不要である。但し、ＣＤ－Ｒ１のファイルシステムとホスト装置２１のファイルシステムとの相互変換を行うためのドライバソフトの類は必須である。ユーザはこのドライバソフトを介してＣＤ－Ｒ記録再生装置１０を利用することにより、ホスト装置２１に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにＣＤ－Ｒ１のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でＣＤ－Ｒ１内の目的とするファイルを利用することができるようになっている。

【００３９】ＣＤ－Ｒ記録再生装置１０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置２１のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ１４を位置させると共に、スピンドルモータ１２の回転速度を制御し、光ピックアップ１４から再生用のレーザ（パワーが０．２ｍＷ程度に抑えられる点を除き記録用のレーザと同じもの）１３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置２１に転送するという一連の動作を実行する。

【００４０】このように、ＣＤ－Ｒ記録再生装置１０は、ＣＤ－Ｒ１への情報の書き込みを行うことができると共に、ＣＤ－Ｒ１に書き込まれた情報の再生も行うことができる。このＣＤ－Ｒ記録再生装置１０は、記録段階でＣＤ－Ｒ１への情報の書き込みを行う場合に必要不可欠な構成要素であるが、再生段階で、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合も必要とされる構成要素である。ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはＣＤ－ＲＯＭ再生装置が搭載されており、そのＣＤ－ＲＯＭ再生装置を利用してＣＤ－Ｒ１の情報再生を行うことも可能であるが、このＣＤ－ＲＯＭ再生装置は、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報や暗号鍵にアクセスできないから、やはり、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合もＣＤ－Ｒ記録再生装置１０は欠かせない構成要素である。

【００４１】また、ＣＤ－Ｒ記録再生装置１０はもっぱらユーザによる記録や再生で使用される装置であるが、ＣＤ－Ｒ１への情報書き込み機能に注目すると、その基本的動作は、ＣＤ－Ｒ１の製造段階で行われるＩＤ情報や暗号鍵の書き込みにも適用可能であるから、以下の説明では上記のＣＤ－Ｒ記録再生装置１０をユーザ段階と製造段階の両方で使用されるものとして話を進める。

【００４２】＜出荷時情報記録処理＞図７は、ＣＤ－Ｒ１の製造段階におけるＩＤ情報と暗号鍵の書き込み動作（以下「出荷時情報記録処理」という。）を示すフローチャートである。なお、製造段階では、ＣＤ－Ｒ記録再生装置１０の記録機能しか利用しないため、図示のフローチャートではＣＤ－Ｒ記録再生装置１０のことを便宜的に「記録機」と称している。但し、この用語（記録機）には、ＣＤ－Ｒ記録再生装置１０に限らず、製造段階専用の“記録機”であってもよい旨の意図も含まれている。

【００４３】図において、出荷時情報記録処理を開始すると、まず、未記録のＣＤ－Ｒ１（フロー中では「ディスク」と称する。）を用意し、このＣＤ－Ｒ１を記録機に装填する（ステップＳ１１）。次に、ホスト装置２１を操作してＣＤ－Ｒ１への記録情報を手入力または自動生成する（ステップＳ１２）。この記録情報はＣＤ－Ｒ１のＩＤ情報や所定の秘密鍵および当日の日付（作成日

付）などであり、そのフォーマットは、図５（ａ）または（ｂ）に示すとおりである。

【００４４】次いで、ホスト装置２１から記録機に対して情報記録命令を発行すると（ステップＳ１３）、記録機はこの命令に応答してレーザ強度キャリブレーション処理を実行し、適正なパワーに記録用レーザ１３を設定した後、光ピックアップ１４をＣＤ－Ｒ１の記録領域の“特定位置”に移動制御する（ステップＳ１４）。この特定位置は原理的にはユーザからの直接的なアクセスが認められていない領域、すなわち、システム領域（ＰＣＡ、ＰＭＡ、リードインまたはリードアウト）の未使用領域上の任意位置である。特に好ましくは、データ再生時にその存在が無視される領域として当業者に広く認知されているＰＣＡまたはＰＭＡ上の（未使用領域上の）任意位置である。以下、説明の便宜上、上記“特定位置”をＰＣＡの未使用領域上の任意位置とする。

【００４５】次いで、記録機は、ホスト装置２１から記録情報（ステップＳ１２で生成した情報）を受け取り、その記録情報を用いて記録用レーザ１３を変調しつつ、記録用レーザ１３をＣＤ－Ｒ１の透明な基板１ｂを介して記録層１ｃの案内溝１ｆに照射し、案内溝１ｆ直下の記録層１ｃに情報ピットを形成して、前記記録情報のＣＤ－Ｒ１への書き込みを行う（ステップＳ１５）。記録情報の書き込み開始位置は、上記ステップＳ１４で実行された光ピックアップ１４の移動位置、すなわち、ＰＣＡの未使用領域上の任意位置であり、記録情報の書き込み終了位置は当該位置から記録情報のサイズ（例えば、図５のフォーマットに従えば２０バイトまたは３６バイト）に相当する分だけ離れた位置である。

【００４６】次いで、記録機は、光ピックアップ１４を上記特定位置に復帰させると共に、当該位置を再生開始位置、記録情報のサイズに相当する分だけ離れた位置を再生終了位置として、システム領域に書き込んだ記録情報の再生を行い、この再生情報をホスト装置２１に転送する。ホスト装置２１は、記録機から転送された再生データと上記記録情報とを比較照合してベリファイ検査を行い（ステップＳ１６）、両者が一致していれば正常に書き込みを行えたと判断してその旨を作業者に報知する一方、そうでなければ書き込みを失敗したと判断してその旨を作業者に報知する（ステップＳ１７）。作業者は、正常書き込み報知の場合に当該ＣＤ－Ｒ１を出荷棚へ移動し（ステップＳ１８）、書き込み失敗報知の場合に当該ＣＤ－Ｒ１を不良品棚へ移動する（ステップＳ１９）。そして、以上の処理を用意されたＣＤ－Ｒ１がなくなるまで繰り返して実行する（ステップＳ２０）。

【００４７】したがって、この「出荷時情報記録処理」によれば、未記録のＣＤ－Ｒ１のシステム領域にＩＤ情報、暗号鍵および作成日付などの隠し情報を書き込んで市場に出荷し、ユーザに届けることができる。そして、ユーザ段階で、以下に説明するデータ書き込み処理、データ再生処理またはディスクコピー処理を行う際に、上記の隠し情報を利用した本実施の形態特有の処理を実行することができる。

【００４８】＜ユーザによるデータ書き込み処理＞図８は、ユーザ段階で実行されるデータ書き込み動作（以下「ユーザによるデータ書き込み処理」という。）を示すフローチャートである。ユーザは上述の「出荷時情報記録処理」を終えたＣＤ－Ｒ１を市場で入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０にセットして、図示の処理を開始する。

【００４９】この処理を開始すると、まず、ホスト装置２１からＣＤ－Ｒ記録再生装置１０へ書き込み命令が発行される。ＣＤ－Ｒ記録再生装置１０はこの命令に応答してＣＤ－Ｒ１のシステム領域からＩＤ情報を読み出し（ステップＳ３１）、サポートディスクであるか否かを判定する（ステップＳ３２）。サポートディスクとは、前述のとおり、所定の製造者またはあらかじめ登録された製造者によって作られたディスクのことである。ＣＤ－Ｒ記録再生装置１０はこれらの製造者を識別するためのＩＤ情報リスト（以下「サポートリスト」という。）を保持しており、上記のステップＳ３２で当該サポートリストを参照してＩＤ情報が登録済みであれば、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクであると判定する。

【００５０】ステップＳ３２の判定結果が“否”（ＮＯ）の場合、すなわち、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクでない場合は、ホスト装置２１に対してサポートディスクへの交換を促す旨のメッセージ（例えば、“このディスクはセキュリティ対応ではありません。セキュリティ対応のディスクに交換してください。”）を送出（ステップＳ３３）して、ディスク交換後の書き込み続行または書き込み中止を判定（ステップＳ３８）する一方、ステップＳ３２の判定結果が“肯”（ＹＥＳ）の場合、すなわち、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１がサポートディスクである場合は、以下の処理を実行する。

【００５１】まず、記録データに機密フラグを付加する（ステップＳ３４）。この機密フラグは、前述のとおり、再生段階において、復号後の平文データの再利用を禁止するためのチェックフラグとして用いられるものであり、好ましくは、電子透かしのような技術を応用してその存在を秘匿化したデータのことである。次いで、ＣＤ－Ｒ記録再生装置１０にセットされているＣＤ－Ｒ１のシステム領域から暗号鍵を読み出し（ステップＳ３６）、その暗号鍵を用いて上記の機密フラグを付加した記録データを暗号化した後、その暗号化データをＣＤ－Ｒ１のユーザ領域に記録する（ステップＳ３７）。

【００５２】最後に、他のＣＤ－Ｒ１に書き込みを行うか否かを判定し（ステップＳ３８）、書き込みを継続す

る場合は、所要のメッセージ（例えば、“新しいディスクをセットしてください”）をホスト装置２１に送出すると共に、書き込み済みのＣＤ－Ｒ１をリジェクトしてステップＳ３１以降を繰り返し、書き込みを継続しない場合は書き込み済みのＣＤ－Ｒ１をリジェクトして処理を終了する。

【００５３】図９は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図である。この図において、ユーザは、ＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置１０に装填すると共に、ホスト装置２１を操作して所要の書き込み命令をＣＤ－Ｒ記録再生装置１０に発行する。ＣＤ－Ｒ記録再生装置１０はこの書き込み命令に応答して、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報を読み出し、所定のＩＤ情報リスト（サポートリスト）と照合してサポートディスクであるか否かを判定する。そして、サポートディスクでなければ、ホスト装置２１に対してディスクの交換を促し、サポートディスクであれば、ホスト装置２１に対してその旨を通知する。ホスト装置２１はサポートディスクである旨の通知に応答して、記録データに機密フラグを付加し、ＣＤ－Ｒ記録再生装置１０に対して暗号鍵を要求する。ＣＤ－Ｒ記録再生装置１０はＣＤ－Ｒ１のシステム領域から暗号鍵を読み出し、その暗号鍵をホスト装置２１に転送する。ホスト装置２１は転送された暗号鍵を用いて記録データ（機密フラグを付加したもの）を暗号化し、その暗号化データをＣＤ－Ｒ記録再生装置１０に転送し、ＣＤ－Ｒ記録再生装置１０は転送された暗号化データをＣＤ－Ｒ１に記録する。

【００５４】したがって、この「ユーザによるデータ書き込み処理」によれば、所定のサポートリストに記載されたＩＤ情報を持つＣＤ－Ｒ、要するに、特定の製造者によって作られたＣＤ－Ｒについてのみ、そのユーザ領域に、機密フラグを付加した記録データを暗号化して記録することができるから、サポートリストに未記載の製造者によって作られたＣＤ－Ｒとの差別化を図ることができ、市場での優位性を得ることができる。

【００５５】＜ユーザによるデータ再生処理＞図１０は、ユーザ段階のデータ再生に用いられる再生専用機（以下「ＣＤ－Ｒ再生装置」という。）の概略的なブロック構成図であり、前述のＣＤ－Ｒ記録再生装置１０（図６参照）との相違は、データの記録機能を持たない点である。すなわち、このＣＤ－Ｒ再生装置３０（発明の要旨に記載のライトワンス型光ディスク用データ再生装置に相当）は、ＣＤ－Ｒ１のクランピングエリアを担持して所定方向に回転駆動するスピンドルモータ３２と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに再生用のレーザ３３を照射する光ピックアップ３４と、光ピックアップ３４の内部に設けられた不図示のシークモータと協調して光ピックアップ３４をディスクの半径方向に移動させる粗動モータ３５とを備えると共に、スピンドルモータ３２の回転速度を制御するディスク回転制御部３６と、粗動モータ３５の回転速度と回転方向を制御する粗動モータ制御部３７と、光ピックアップ３４の位置やレーザ強度の制御を行うピックアップ制御部３８と、光ピックアップ３４からの読み取り信号の波形変換等の制御を行う再生制御部３９とを備え、さらに、これらの各制御部を統括するコントローラ４０を備える。

【００５６】このＣＤ－Ｒ再生装置３０は、前述のＣＤ－Ｒ記録再生装置１０と同様に、パーソナルコンピュータ等のホスト装置５１の拡張スロットに内蔵され（または外付けされ）、ホスト装置５１とコントローラ４０との間を所定の信号規格（例えば、ＳＣＳＩ）のケーブル５１ａで接続して用いられる。

【００５７】このような構成を有するＣＤ－Ｒ再生装置３０は、以下に示すとおり、ＣＤ－Ｒ１に書き込まれた情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ再生装置３０は、先に説明したＣＤ－Ｒ記録再生装置１０と同様にＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００５８】図１１は、ホスト装置５１の階層的機能概念図であり、図示の階層構造は、いわゆるＯＳＩ（Open System Interconnection：開放型システム間相互接続）参照モデルと同様に最下位層を物理層、最上位層をアプリケーション層とする構造を有している。この構造は大きく分けて、物理層と密接に関係するドライバ層５１ｂと、その上位に位置するいわゆるオペレーティングシステム（ＯＳ）によって提供されるサービス層５１ｃと、最上位層に位置してユーザインターフェースを実現するためのアプリケーション層５１ｄとからなり、アプリケーション層５１ｄに実装されたアプリケーションプログラム（例えば、ＣＤ－Ｒ再生装置３０を利用するためのユーザインターフェースを含むもの）５１ｅは、サービス層５１ｃのオペレーティングシステム５１ｆのＡＰＩ（Application Programmable Interface）を介してドライバ層５１ｂにアクセスし、例えば、ＣＤ－Ｒ再生装置３０をはじめとした各種リソースを利用する。

【００５９】ここで、ドライバ層５１ｂには多種多様なドライバプログラムが実装されている。例えば、ＣＤ－Ｒ再生装置３０のインターフェース規格をＳＣＳＩとすると、少なくともＳＣＳＩドライバ（ＡＴＡＰＩドライバともいう）５１ｇやＳＣＳＩポート用のミニポートドライバ５１ｈおよび入出力制御用のＩＯＳ（Input／Output Supervisor）ドライバ５１ｉなどが実装されている。

【００６０】一般にアプリケーションプログラム５１ｅはオペレーティングシステム５１ｆの所定のＡＰＩを利用して、物理層に位置する各種リソースを利用するが、通常、アプリケーションプログラム５１ｅから見て、これらのドライバの存在は意識されない。例えば、アプリ

ケーションプログラム５１ｅからＣＤ－Ｒ再生装置３０を利用する場合、実際には、ＩＯＳドライバ５１ｉやＳＣＳＩドライバ５１ｇおよびミニポートドライバ５１ｈを間接的に利用している。また、ファイルコピーの操作などを行う場合も、実際にはＩＯＳドライバ５１ｉを間接的に利用している。

【００６１】ところで、図示のドライバ層５１ｂには、ハッチングで他と区別された特別なドライバ（以下「フィルタドライバ」という。）５１ｊが実装されている。このフィルタドライバ５１ｊは本実施形態に特有のもので、少なくとも（ａ）アプリケーションプログラム５１ｅの要求に応じてＣＤ－Ｒ再生装置３０からオペレーティングシステム５１ｆに渡されるデータをモニタし、そのデータ内に前述の“機密フラグ”が含まれているか否かを判定する第一の機能と、（ｂ）上記“機密フラグ”の存在を判定した場合に当該データに対するオペレーティングシステム５１ｆのコピー動作や保存動作を拒否ないしは制限（例えば、コピー命令や保存命令を無視したりすること）する第二の機能とを持つものであり、発明の要旨に記載の判定手段および禁止手段に相当するものである。

【００６２】第一の機能を実現するために、フィルタドライバ５１ｊはＳＣＳＩドライバ５１ｇとミニポートドライバ５１ｈの間に実装されており、さらに、第二の機能を実現するために、オペレーティングシステム５１ｆとＩＯＳドライバ５１ｉの間に実装されている。なお、この実装位置は一例である。要はアプリケーション層５１ｄから直接的にアクセスできない位置であって、且つ、上記モニターと上記コピー動作や保存動作の拒否に適した位置に実装されていればよい。また、フィルタドライバ５１ｊは図示のように単一のものでなく、各機能ごとに分割されたものであってもよい。

【００６３】ユーザは、アプリケーションプログラム５１ｅによって提供されるユーザインターフェースを操作しながらＣＤ－Ｒ再生装置３０にアクセスし、ＣＤ－Ｒ１に記録されたデータの再生を行う。この再生処理に際して、オペレーティングシステム５１ｆやドライバプログラム５１ｇ～５１ｊは黒子的な仲介役となって表に出てこない。すなわち、ユーザは、オペレーティングシステム５１ｆやドライバプログラム５１ｇ～５１ｊの存在を意識することなく、ＣＤ－Ｒ再生装置３０にアクセスし、ＣＤ－Ｒ１に記録されたデータを利用することができる。

【００６４】ＣＤ－Ｒ１に記録されたデータは、アプリケーションプログラム５１ｅから見て、オペレーティングシステム５１ｃのファイルシステムによって管理された独立したデータの集まり（ファイル）として認識される。ユーザは、このデータを他の記憶デバイスに格納されたデータと同様に取り扱う（ファイルアクセス）ことができる。ＣＤ－Ｒ再生装置３０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置５１のドライバ層５１ｂに提供すると共に、当該ドライバソフト層５１ｂから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ３４を位置させると共に、スピンドルモータ３２の回転速度を制御し、光ピックアップ３４から再生用のレーザ３３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置５１のドライバ層５１ｂに転送するという一連の動作を実行する。

【００６５】図１２は、ユーザ段階で実行されるデータ再生動作（以下「ユーザによるデータ再生処理」という。）を示すフローチャートである。ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ再生装置３０にセットして、そのＣＤ－Ｒ１からＩＤ情報を読み出す（ステップＳ４１）と共に、ホスト装置５１に対してＩＤ入力を要求する（ステップＳ４２）。ホスト装置５１は、画面上にＩＤ入力を促す旨の所定のＧＵＩ（Graphical User Interface）を表示してユーザによるキーボード等からのＩＤ入力を受け付け、入力されたＩＤ情報をＣＤ－Ｒ記録再生装置１０に転送する。ＣＤ－Ｒ再生装置３０は、転送されたＩＤ情報とＣＤ－Ｒ１から読み込んだＩＤ情報とを比較し（ステップＳ４３）、一致した場合は正規ユーザ、一致しなかった場合は不正なユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、以下の処理を実行する。

【００６６】まず、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵と暗号化データを読み出して（ステップＳ４４、ステップＳ４５）、ホスト装置５１に転送する。ホスト装置５１は、転送されたデータに機密フラグが含まれているか否かを判定し（ステップＳ４６）、含まれている場合は、暗号鍵を用いてその暗号化データを復号し（ステップＳ４７）、平文のデータに戻してユーザの利用に供する一方、機密フラグが含まれていない場合は、復号動作を行うことなく、そのまま処理を終了する。

【００６７】図１３は、上記「ユーザによるデータ再生処理」のタイムランを示す図である。この図において、ユーザは、ＣＤ－Ｒ１をＣＤ－Ｒ再生装置３０に装填すると共に、ホスト装置５１を操作して所要の再生命令をＣＤ－Ｒ再生装置３０に発行する。ＣＤ－Ｒ再生装置３０はこの再生命令に応答してＩＤ要求をホスト装置５１に返し、ホスト装置５１は画面上にＩＤ入力を促す旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ１の配布先から正当に通知された

ＩＤ情報）を入力し、ホスト装置５１は入力されたＩＤ情報をＣＤ－Ｒ再生装置３０に転送する。

【００６８】ＣＤ－Ｒ再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出し、ホスト装置５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置５１に転送する。ホスト装置５１は、転送データ中に機密フラグがあるか否かを判定し、機密フラグが含まれている場合は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容する一方、機密フラグが含まれていない場合は復号動作を行うことなく、処理を終了する。

【００６９】したがって、この「ユーザによるデータ再生処理」によれば、ＣＤ－Ｒのシステム領域に書き込まれているＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができ、正規ユーザによってデータ再生処理が行われている場合に、ＣＤ－Ｒのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送することができる。そして、転送データ中に機密フラグが含まれている場合に、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を当該正規ユーザに許容することができる。

【００７０】その結果、不正ユーザを排除してデータの再生を行うことができると共に、機密フラグが含まれている暗号化データの復号のみを行うことができるから、前記の「ユーザによるデータ書き込み処理」との組み合わせによって、記録段階から再生段階までの一連のセキュリティ対策を確立することができるうえ、このセキュリティ対策に欠くことのできない記録媒体として特定の製造者によって作られたサポートディスクの使用を強制することができる。

【００７１】＜ユーザによるディスクコピー処理＞図１４は、ユーザ段階で実行されるデータコピー動作（以下「ユーザによるデータコピー処理」という。）を示すフローチャートである。なお、以下の説明では、データのコピー先をＣＤ－Ｒとしているが、これはデータ再利用の一例であり、コピー先は如何なる記憶媒体であってもかまわない。ハードディスクやその他の記録媒体であってもよい。

【００７２】図１４において、ユーザによるデータコピー処理を開始すると、ユーザは、前述のユーザによるデータ書き込み処理によって暗号化データ（記録データに機密フラグを付加して暗号化したもの）が書き込まれたＣＤ－Ｒ１をコピー元、未記録のＣＤ－Ｒをコピー先とし、それぞれをコピー元のＣＤ－Ｒ再生装置３０とコピー先のＣＤ－Ｒ記録再生装置１０にセットする。そして、ホスト装置５１を操作してコピー元のＣＤ－Ｒ再生装置３０にコピー命令を発行する。コピー元のＣＤ－Ｒ再生装置３０は、コピー命令に応答してＣＤ－Ｒ１からＩＤ情報を読み出す（ステップＳ５１）と共に、ホスト装置５１に対してＩＤ入力を要求する（ステップＳ５２）。ホスト装置５１は画面上にＩＤ入力を促す旨の所定のＧＵＩを表示してユーザによるキーボード等からのＩＤ入力を受け付け、入力されたＩＤ情報をコピー元のＣＤ－Ｒ再生装置３０に転送する。

【００７３】コピー元のＣＤ－Ｒ再生装置３０は、転送されたＩＤ情報とＣＤ－Ｒ１から読み込んだＩＤ情報とを比較し（ステップＳ５３）、一致した場合は正規ユーザ、一致しなかった場合は不正ユーザと判断し、不正ユーザの判断時にはそのまま処理を終了する一方、正規ユーザの判断時には、コピー元のＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵と暗号化データを読み出してホスト装置５１に転送する。ホスト装置５１は、そのドライバ層５１ｂに実装されたフィルタドライバ５１ｊにより、転送データ中に機密フラグが存在するか否かを判断し（ステップＳ５４）、機密フラグが存在しなければ、転送された暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のＣＤ－Ｒ記録再生装置１０に転送してコピー先のＣＤ－Ｒ１に記録するというコピー処理を実行（ステップＳ５５）して処理を終了する一方、機密フラグが存在していれば、同コピー処理を強制的に中止（ステップＳ５６）して処理を終了する。

【００７４】図１５は、上記「ユーザによるデータコピー処理」のタイムランを示す図であり、図中のＣＤ－Ｒ１とＣＤ－Ｒ再生装置３０はコピー元のもの、ＣＤ－Ｒ記録再生装置１０とＣＤ－Ｒ１′はコピー先のものである。この図において、ユーザは、コピー元とコピー先のＣＤ－Ｒ１、１′をそれぞれＣＤ－Ｒ再生装置３０とＣＤ－Ｒ記録再生装置１０に装填すると共に、ホスト装置５１を操作して所要のコピー命令をコピー元のＣＤ－Ｒ再生装置３０に発行する。コピー元のＣＤ－Ｒ再生装置３０はこのコピー命令に応答してＩＤ要求をホスト装置５１に返し、ホスト装置５１は画面上にＩＤ入力を促す旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ１の配布先から正当に通知されたＩＤ情報）を入力し、ホスト装置５１は入力されたＩＤ情報をコピー元のＣＤ－Ｒ再生装置３０に転送する。

【００７５】コピー元のＣＤ－Ｒ再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出し、ホスト装置５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を終了する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ１に書き込まれている暗号鍵と暗号化データとを読み出してホスト装置５１に転送する。ホスト装置５１は、そのドライバ層５１ｂに実装されたフィルタ

ドライバ５１ｊにより、転送データ中の機密フラグの存在を判断する。そして、存在していればコピー処理を強制的に中止する一方、存在していなければ、暗号鍵を用いて暗号化データを復号し、その復号データをコピー先のＣＤ－Ｒ記録再生装置１０に転送し、コピー先のＣＤ－Ｒ記録再生措置１０はその転送データをＣＤ－Ｒ１′に書き込む。

【００７６】したがって、この「ユーザによるデータコピー処理」によれば、コピー元のＣＤ－Ｒのシステム領域に書き込まれているＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができると共に、機密フラグが付加されたデータのコピーが行われようとした場合は、たとえ正規ユーザであっても、そのコピー動作を強制的に中止（コピー動作の拒否）して実行しないようにすることができる。その結果、暗号化データに機密フラグが存在する場合は、コピー処理を積極的に禁止できるから、復号データの再利用を阻止することができ、記録から再生までのすべての段階にわたってセキュリティを持たせることができる。

【００７７】＜まとめ＞以上、説明したとおり、本実施の形態によれば、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報を用いて、サポートリストに記載された製造者のＣＤ－Ｒ１（サポートディスク）であるか否かを判定でき、サポートディスクの場合に所定の機密フラグを付加した記録データを暗号化してＣＤ－Ｒ１に記録することができる。そして、再生側でこの暗号化データを読み出す際に、機密フラグの有無を検査し、機密フラグがある場合に復号データの再利用を禁止することができる。したがって、ホスト装置５１の内部には、前述の「ユーザによるデータ再生処理」によってメインメモリ上に一時的に作られた復号データしか存在しないため、しかも、この一時的データはプロセスからの利用完了時点で速やかに解放されるため、再利用可能な復号データの痕跡が残されることはなく、データの不正流出等を確実に防止することができるという格別有益な効果が得られる。

【００７８】なお、以上の説明では、ＩＤ情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のＰＣＡやＰＭＡはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【００７９】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のＤＥＳ方式以外にも、ＦＥＡＬ：Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバヘッドおよび暗号化データのボリューム等を勘案して適切な方式を採用すればよい。

【００８０】また、前記説明のセキュリティ機能のうち、特に復号データの再利用を禁止する機能は、もっぱらホスト装置５１に実装されたフィルタドライバ５１ｊやその他の汎用ドライバおよびオペレーティングシステム等のソフトウェアリソースと、ホスト装置５１の各種ハードウェアリソースとの有機的結合によって機能的に実現されるものであるが、フィルタドライバ５１ｊ以外のリソースは汎用のものを利用できるから、前記説明の「復号データの再利用を禁止する機能」にとって欠くことのできない必須の事項は、実質的に、フィルタドライバ５１ｊのプログラムに集約されているということがいえる。したがって、本発明に係るセキュリティ機能のポイントは、それらのプログラムのすべてまたはその要部を格納した、フロッピィディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む構成品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または構成品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

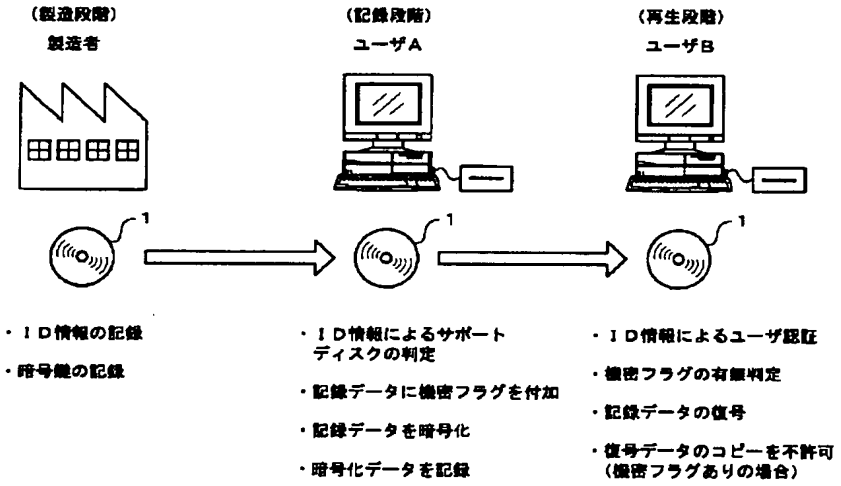
【００８１】また、以上の説明では、ライトワンス型光ディスクとしてＣＤ－Ｒの例を示したが、これに限らない。例えば、ＤＶＤ（Digital Video DiscまたはDigital Versatile Disc）－Ｒも１回だけのデータ書き込みを行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をＤＶＤ－Ｒに適用する場合、ＣＤ－ＲをＤＶＤ－Ｒと読み替えると共に、ＣＤ－Ｒ記録再生装置やＣＤ－ＲライターをそれぞれＤＶＤ－Ｒ記録再生装置、ＤＶＤ－Ｒライターと読み替えればよい。

【００８２】

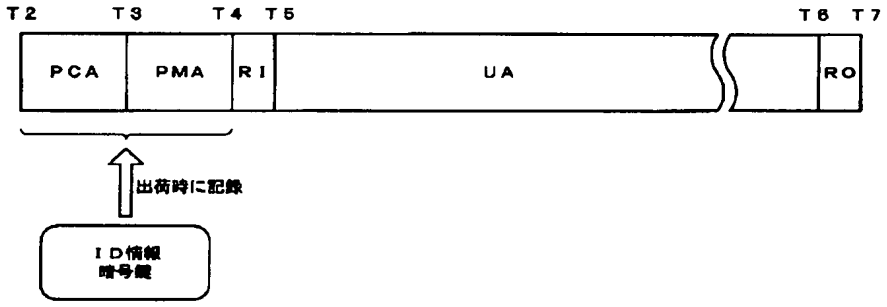
【発明の効果】請求項１記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が制限される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項２記載の発明によれば、光ディスクのシステム領域に不可視状態で格納されたセキュリティ情報に基づいて光ディスクへのアクセスが制限される。したがって、例えば、データ再生時に正当なユーザを認証して書き込みデータへのアクセスを許容することができ、不正ユーザの排除等、セキュリティ性の向上を図ることができる。請求項３記載の発明によれば、データの再生時に所定の機密フラグが検出されると、再生データの複製物の生成が禁止される。したがって、再生データの再利用を阻止して、再生段階におけるセキュリティを確保することができる。請求項４記載の発明によれば、マイクロコンピュータを含むハードウェアリソースと該プログラムとの有機的結合によって前記判定手段および禁止手段を実現できる。

【図面の簡単な説明】
【図１】本実施形態のＣＤ－Ｒの利用模式図である。
【図２】ライトワンス型光ディスクの外観図およびその要部拡大図である。
【図３】ＣＤ－Ｒの断面構造図である。
【図４】ＣＤ－Ｒの各記録領域のフォーマット概念図である。
【図５】ＣＤ－Ｒのシステム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。
【図６】ＣＤ－Ｒ記録再生装置の概略的なブロック構成図である。
【図７】出荷時情報記録処理を示すフローチャートである。
【図８】ユーザによるデータ書き込み処理を示すフローチャートである。
【図９】ユーザによるデータ書き込み処理のタイムランを示す図である。
＊【図１０】ＣＤ－Ｒ再生装置の概略的なブロック構成図である。
【図１１】ホスト装置の階層的機能概念図である。
【図１２】ユーザによるデータ再生処理を示すフローチャートである。
【図１３】ユーザによるデータ再生処理のタイムランを示す図である。
【図１４】ユーザによるディスクコピー処理を示すフローチャートである。
【図１５】ユーザによるディスクコピー処理のタイムランを示す図である。
【図１６】従来のセキュリティ対策の概念図である。
【符号の説明】
ＰＣＡ　Power Calibration Area（システム領域）
１　ＣＤ－Ｒ（ライトワンス型光ディスク）
３０　ＣＤ－Ｒ再生装置（ライトワンス型光ディスク用データ再生装置）
＊　５１ｊ　フィルタドライバ（判定手段、禁止手段）

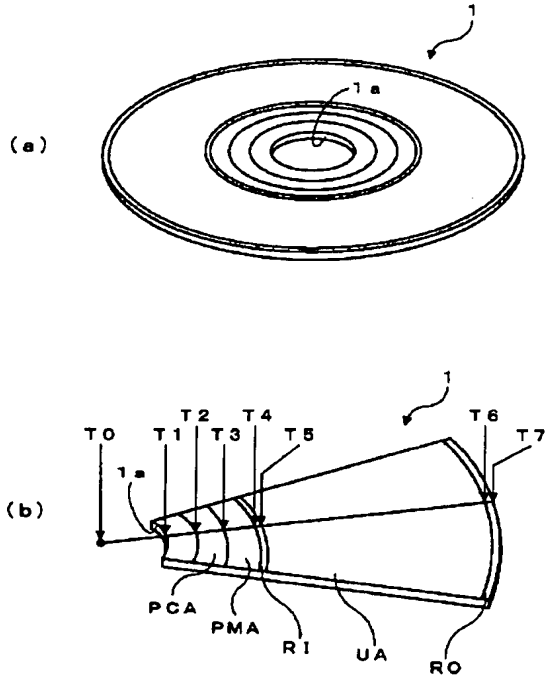
【図１】



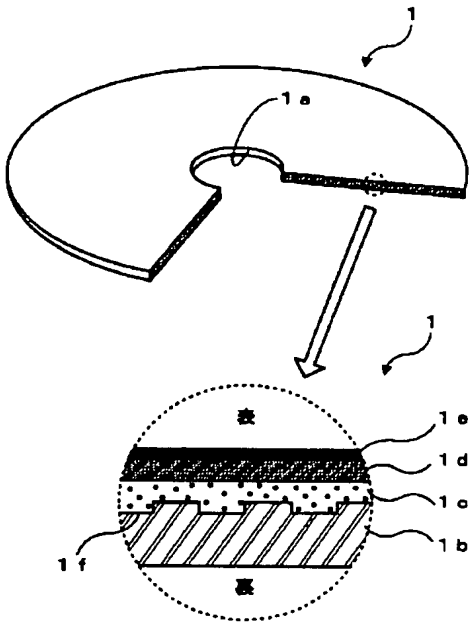
【図４】



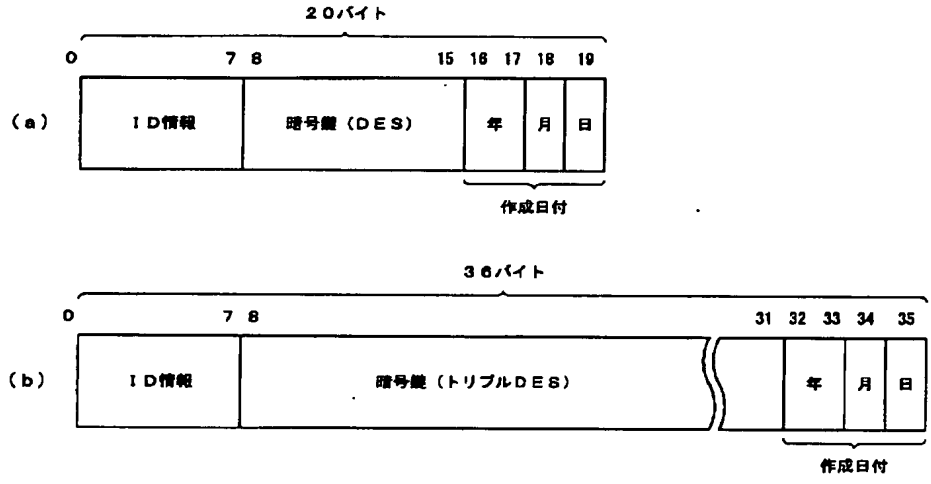
【図２】


(a)
1
1a
(b)
T0
T1
T2
T3
T4
T5
T6
T7
PCA
PMA
RI
UA
RO

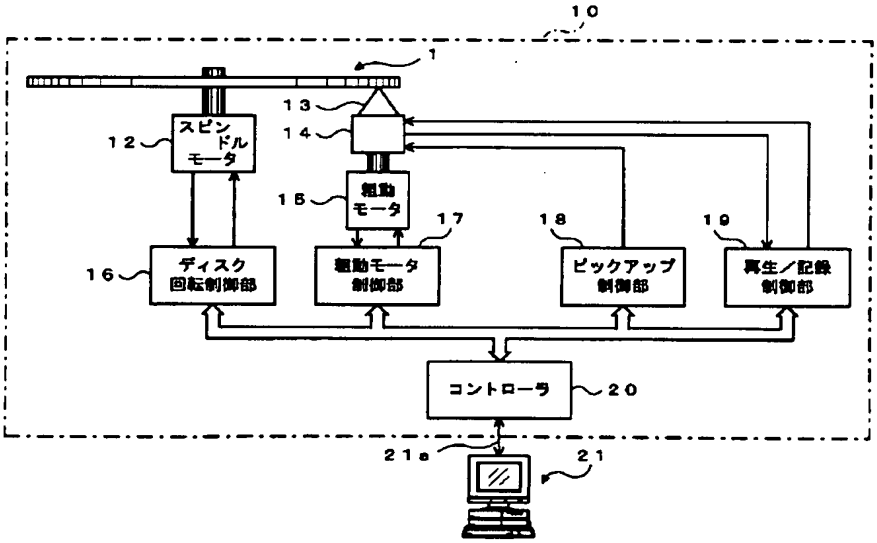
【図３】


1
1a
表
1e
1d
1c
1b
1f
裏

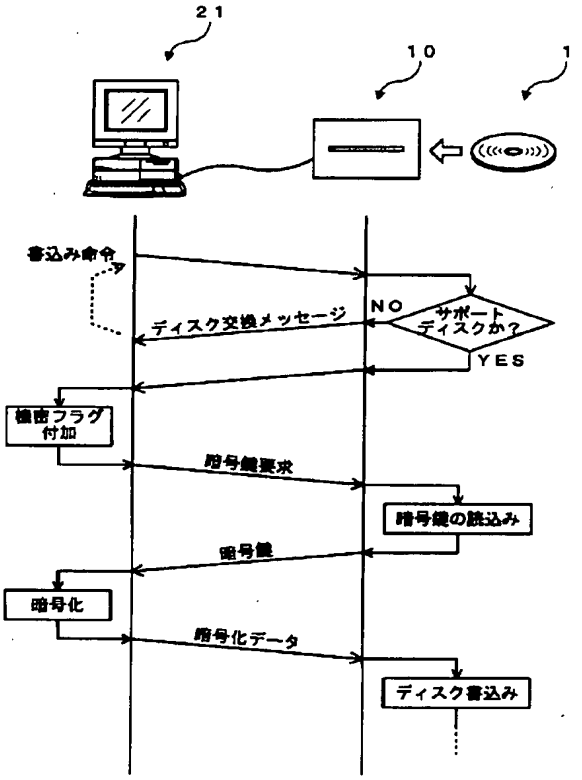
【図５】


20バイト
0
7 8
15 16 17 18 19
(a)
ID情報
暗号鍵（DES）
年
月
日
作成日付
36バイト
0
7 8
31 32 33 34 35
(b)
ID情報
暗号鍵（トリプルDES）
年
月
日
作成日付

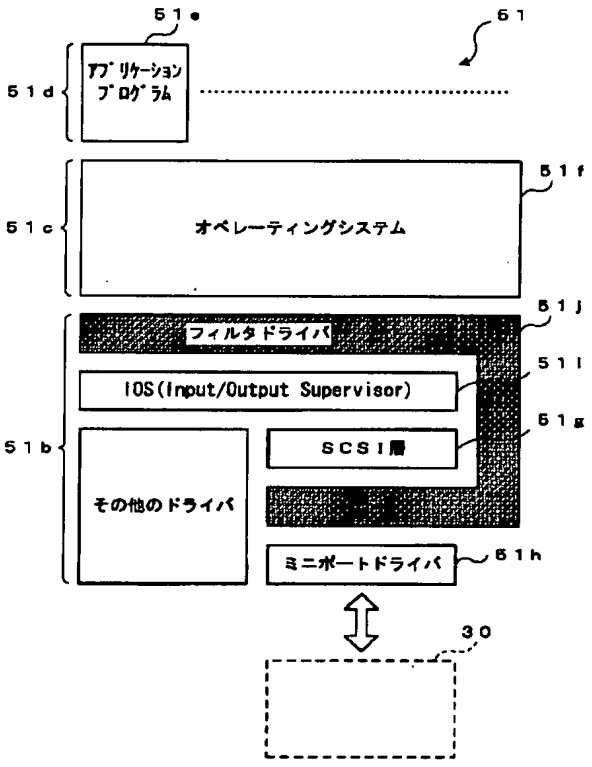
【図６】


10
1
13
12
スピンドルモータ
14
15
粗動モータ
17
18
19
16
ディスク回転制御部
粗動モータ制御部
ピックアップ制御部
再生／記録制御部
コントローラ
20
21a
21

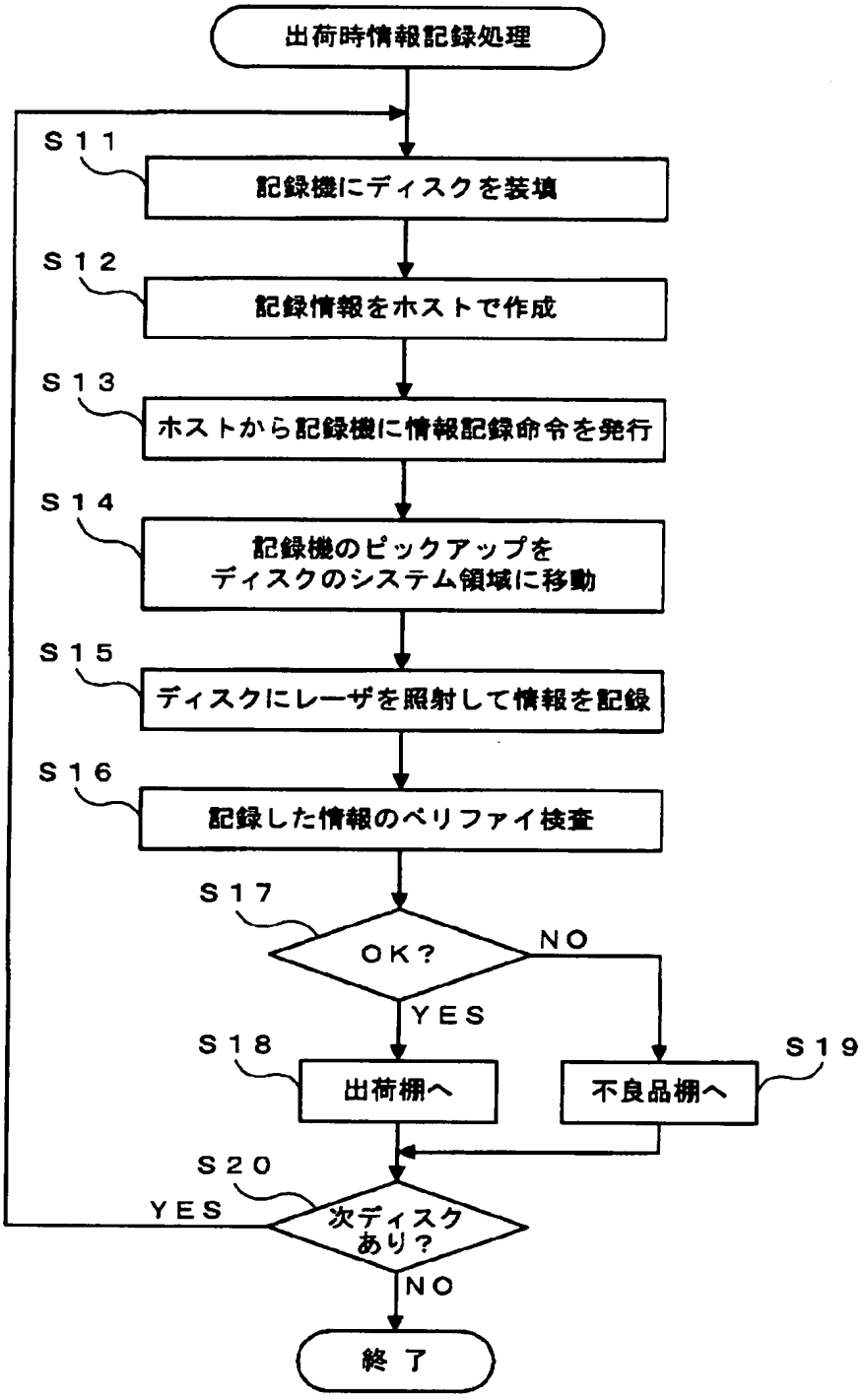
【図９】


21
10
1
書込み命令
ディスク交換メッセージ
NO
サポートディスクか？
YES
機密フラグ付加
暗号鍵要求
暗号鍵の読込み
暗号鍵
暗号化
暗号化データ
ディスク書込み

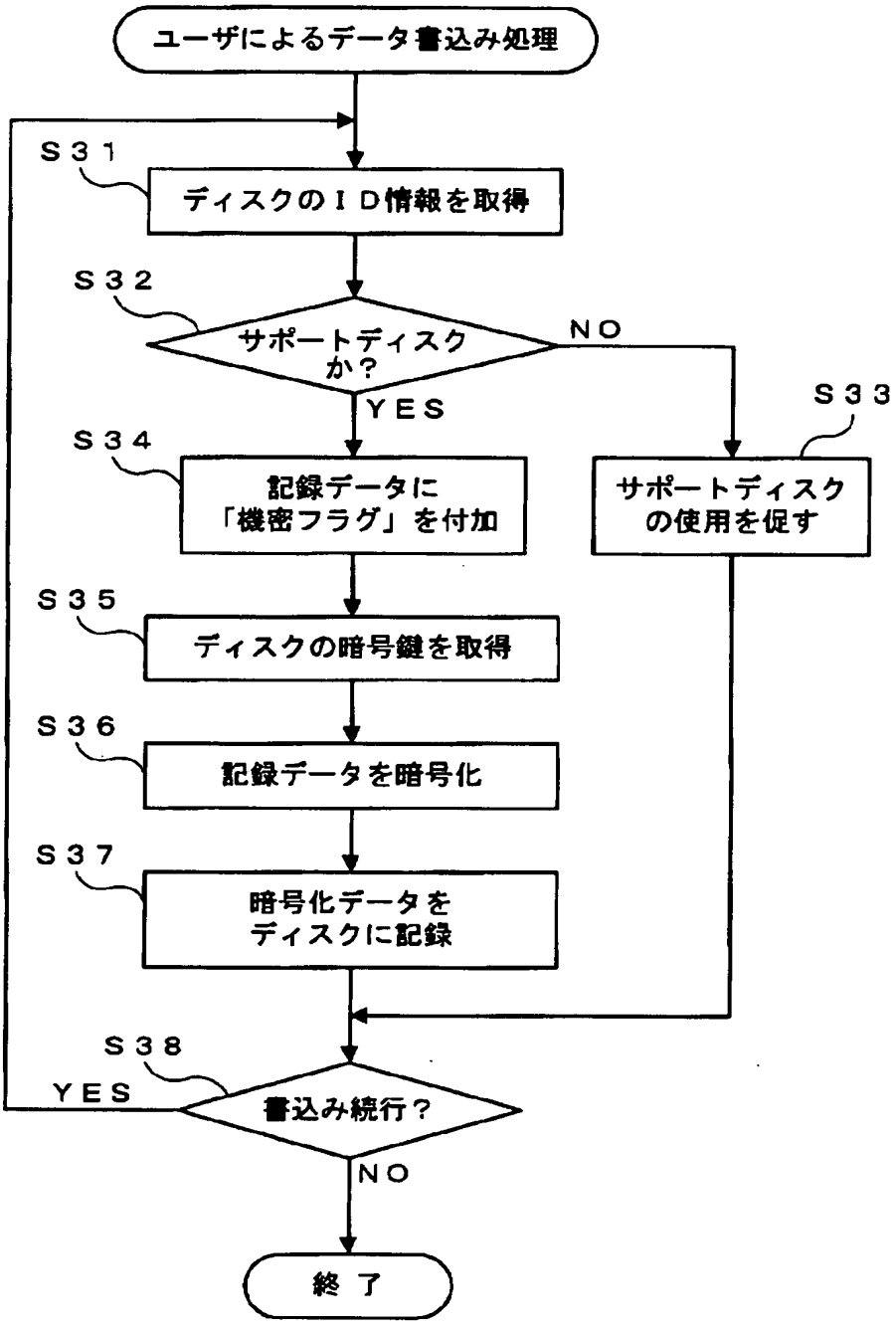
【図１１】


51e
51
51d
アプリケーションプログラム
51f
51c
オペレーティングシステム
51j
フィルタドライバ
51i
IOS(Input/Output Supervisor)
51g
51b
SCSI層
その他のドライバ
ミニポートドライバ
51h
30

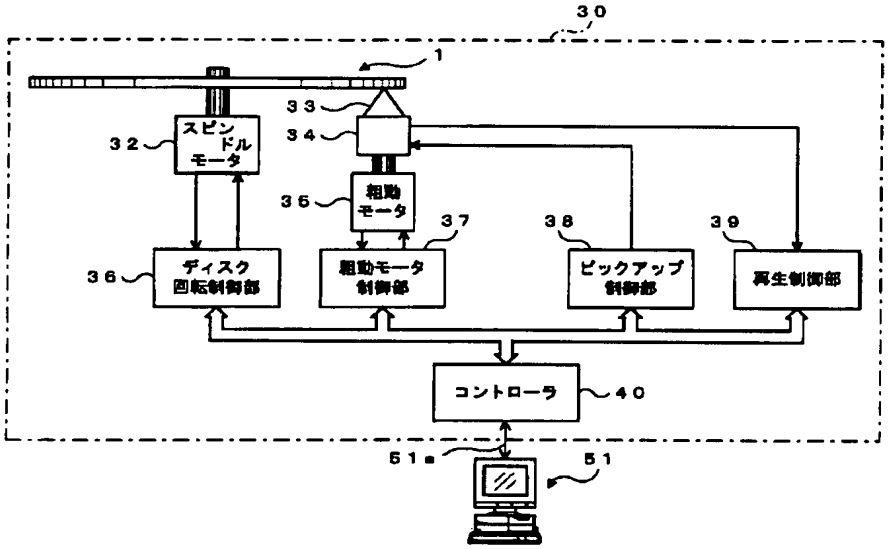
【図７】


出荷時情報記録処理
S11
記録機にディスクを装填
S12
記録情報をホストで作成
S13
ホストから記録機に情報記録命令を発行
S14
記録機のピックアップを
ディスクのシステム領域に移動
S15
ディスクにレーザを照射して情報を記録
S16
記録した情報のベリファイ検査
S17
OK？
NO
YES
S18
出荷棚へ
S19
不良品棚へ
S20
次ディスク
あり？
YES
NO
終了

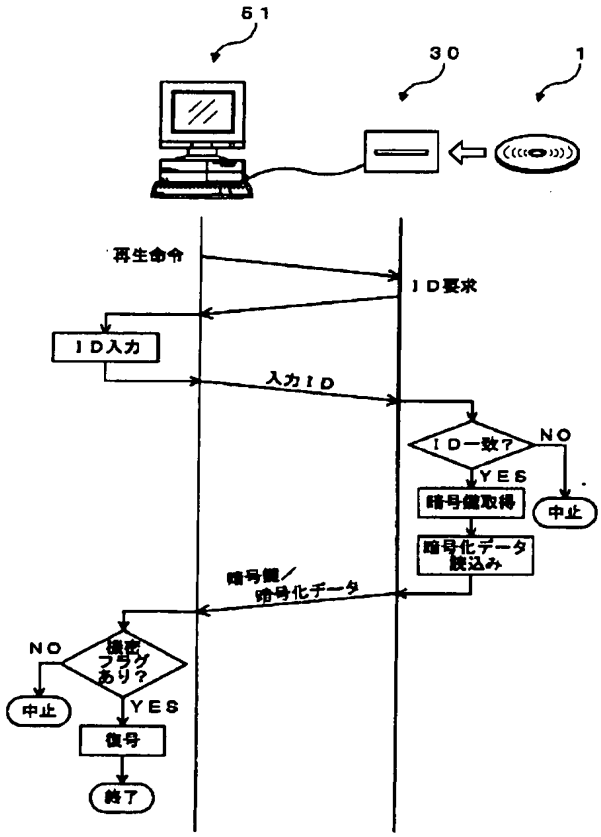
【図８】


ユーザによるデータ書込み処理
S31
ディスクのＩＤ情報を取得
S32
サポートディスクか？
NO
YES
S33
サポートディスクの使用を促す
S34
記録データに「機密フラグ」を付加
S35
ディスクの暗号鍵を取得
S36
記録データを暗号化
S37
暗号化データをディスクに記録
S38
YES
書込み続行？
NO
終了

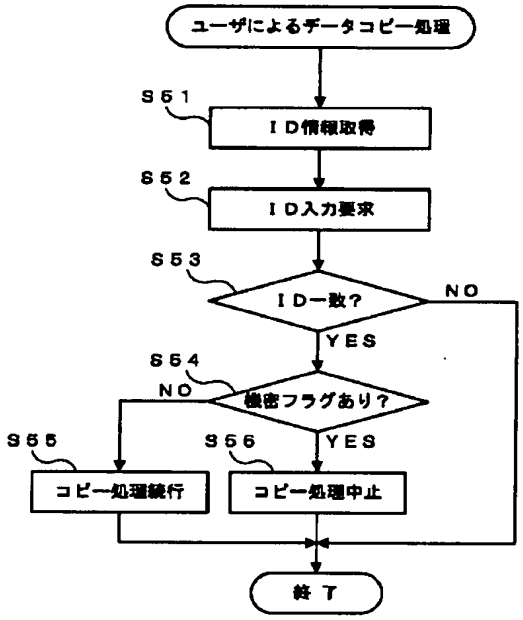
【図１０】


30
1
33
34
32
スピンドルモータ
35
粗動モータ
37
38
39
36
ディスク回転制御部
粗動モータ制御部
ピックアップ制御部
再生制御部
コントローラ
40
51
51

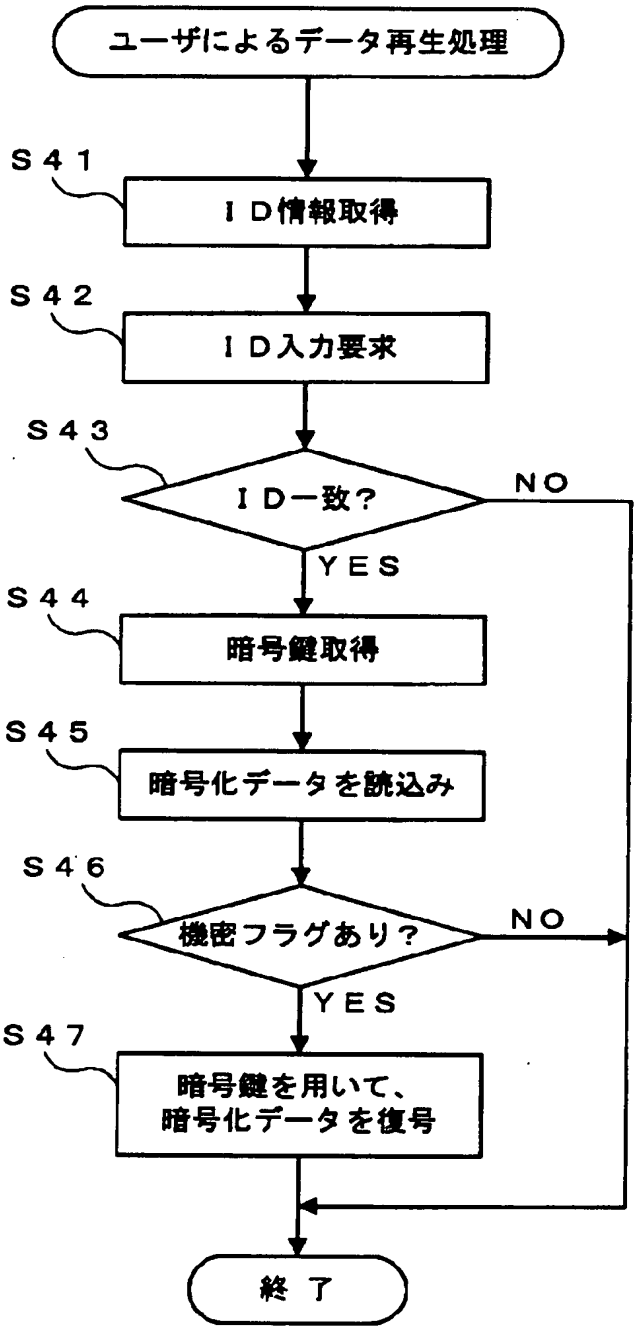
【図１３】


51
30
1
再生命令
ＩＤ要求
ＩＤ入力
入力ＩＤ
ＩＤ一致？
NO
YES
暗号鍵取得
中止
暗号化データ読込み
暗号鍵／暗号化データ
NO
機密フラグあり？
YES
中止
復号
終了

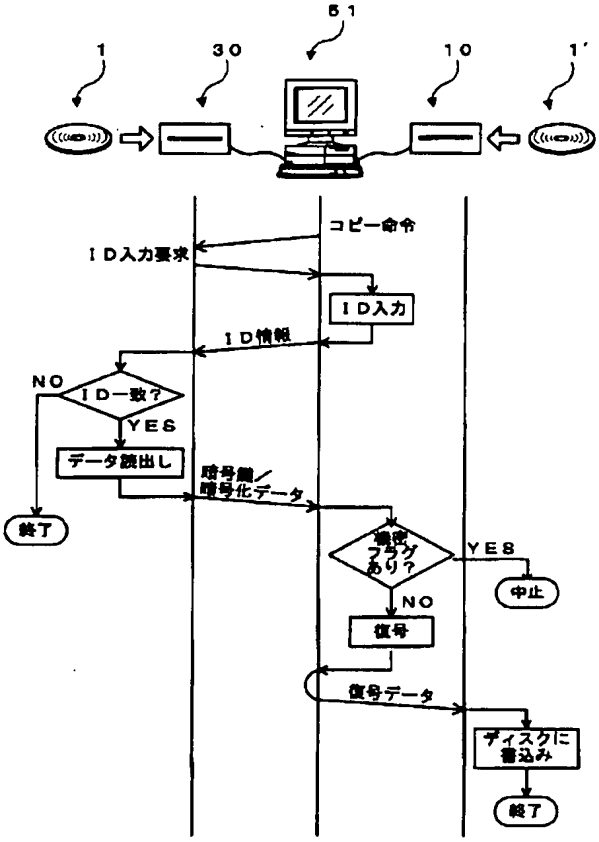
【図１４】


ユーザによるデータコピー処理
S51
ＩＤ情報取得
S52
ＩＤ入力要求
S53
ＩＤ一致？
NO
YES
S54
NO
機密フラグあり？
S55
S56
YES
コピー処理続行
コピー処理中止
終了

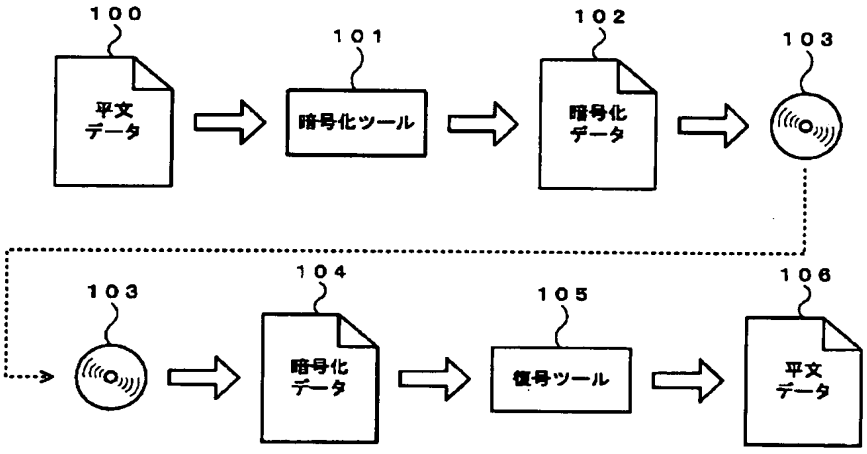
【図１２】


ユーザによるデータ再生処理
S41
ＩＤ情報取得
S42
ＩＤ入力要求
S43
ＩＤ一致？
NO
YES
S44
暗号鍵取得
S45
暗号化データを読込み
S46
機密フラグあり？
NO
YES
S47
暗号鍵を用いて、
暗号化データを復号
終了

【図１５】


51
1
30
10
1'
コピー命令
ＩＤ入力要求
ＩＤ入力
ＩＤ情報
NO
ＩＤ一致？
YES
データ読出し
暗号鍵／
暗号化データ
終了
機密フラグあり？
YES
中止
NO
復号
復号データ
ディスクに書込み
終了

【図１６】



フロントページの続き

(72)発明者　清水　洋信
東京都台東区上野６丁目16番20号　太陽誘電株式会社内

Ｆターム(参考)　5D044 BC05 CC04 DE17 DE60 EF05 FG18 GK12 HL08